DRAFT REQUEST FOR PROPOSAL (RFP)

FOR

e-PROCUREMENT SOLUTION (EPS)

FOR

ACQUISITIONS PROGRAM – PUBLIC WORKS AND GOVERNMENT SERVICES CANADA (PWGSC)

Table of Contents

List of Annexes to the Resulting Contract:
Annex 1 – Statement of Work (SOW)
Annex 2 – Security and Privacy
Annex 3 – Price Schedule
Annex 4 – Security Requirements Check List (SRCL) and Security Classification Guide (SCG)
Annex 5 – Glossary
Annex 6 – Acronyms
Annex 7 – Task Authorization Form

List of Attachments to Part 2 of the RFP:
Attachment 1 to Part 2 – EPS Business Process Modeling Information

List of Attachments to Part 4 of the RFP:
Attachment 1 to Part 4 – Evaluation and Selection Methodology
Attachment 2 to Part 4 – Technical Evaluation
Attachment 3 to Part 4 – Usability Assessment
Attachment 4 to Part 4 – Supply Chain Scope Diagram
Attachment 5 to Part 4 – Financial Evaluation

List of Forms to Part 4 of the RFP:
Form 1 to Part 4 – RFP Submission Form
Form 2 to Part 4 – Project Reference Check Form
Form 3 to Part 4 – SCSI - IT Product List and Subcontractor List Form

Notice to Bidders: National Security Exception (NSE) Notice

All aspects of this solicitation and resulting contract are subject to the national security exception and are, therefore, excluded from all of the obligations of the trade agreements.

1 PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation and resulting contract document is divided into the following parts:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides the Bidder with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: describes how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications: includes the certifications to be provided;

Part 6 Security, Financial and Other Requirements: describes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: describes the clauses and conditions that will apply to any resulting contract.

Refer to the Table of Content for the list of annexes, attachments and forms.

1.2 Summary

1.2.1 Public Works and Government Services Canada (PWGSC) is seeking an e-Procurement Solution (EPS) whereby the service provider will not only be required to deliver an enterprise-wide, commercially available electronic procurement system but also to provide a fully managed service including system configuration, implementation, maintenance, upgrades and operation to ensure Government of Canada's objectives and service level requirements are fully met. The EPS will provide a full range of e-procurement services including but not limited to:

a. Sourcing management;
b. Procurement management;
c. Contract management;
d. Business intelligence; and
e. Supplier relationship management.

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

1.4 Conflict of Interest

1.4.1 Bidders are advised to refer to Conflict of Interest provisions at Article 18 of SACC 2003, Standard Instructions – Goods or Services – Competitive Requirements (dated 2015-07-03) and Conflict of Interest provisions of SACC 2035, General Condition – Higher Complexity – Services (dated 2015-07-03) available on the PWGSC Website **https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual** .

1.4.2 Without limiting in any way the provisions described in 1.4.1 above, Bidders are advised that since April 9, 2014 Canada has engaged the assistance of the following private sector contractors and resources who have provided services including the review of content in preparation of this RFP and/or who have had, or may have had, access to information related to the content of the RFP or other documents related to the EPS solicitation:

Contractors:

Fujitsu Consulting	KPMG LLP
Gartner Canada Co.	Maplesoft Group
Groupe Intersol Group Ltée.	MDOS Consulting Inc., INVA Corporation, KOZA Technology Consulting Inc., in Joint Venture (o/a AGM in Joint Venture)
Hallux Consulting	Phase 5 Consulting Group Inc.
Ian Martin Limited	S.i. Systems
IBISKA	TeraMach Technologies
IT/Net	

Resources (last name, first name):

Alexander, Jim	DuBois, Howard	Mayrand, Richard
Badea, Georgiana	Dufort, Marie-Pier	McLagan, Melanie
Baker, Philip	Duthie, Donald	Peter, Sandra
Benjamin, Jacquie	Fino, Juan	Qureshi, Rehan
Bokor, Charles Villanyi	Fischer, Marian	Rishi, Ripu Daman
Boucher, Michael	Fontaine, François	Rolland, Guillaume
Brulet, Lionel	Gilmour, Ian	Saadany, Ahmed El
Bryson, Richard	Girard, Sylvie	Savoie, Grégoire
Burrill, Gordon	Gladish, Bill	Secretain, Pierre
Carter, Christopher	Haecker, Marcus	Sibley, Robert
Caughlin, Carol	Harris, Richard	Somerville, Anne
Chen, Lian	Kraya, Mohammad	Sourour, Nabil
Choi, Thomas	Krsmanovic, Milenko	Tardiff, Michelle

Cooper, John F	Lamorie, Genevieve	Thérésy, Aude
Côté Raymond	Lechasseur, Guillaume	Thirion, Jérôme
Côté, Larry	Leier, Lynne	Tom, Eva
Croucher, Laura	Letarte, Jean-François	Tworkowski, Krzysztof
Dean, Bryan	Lourdel, Olivier	Wong, Peter
Dennler, Jeff	Lukic, Zack	Woodworth, Gary
Dorica, Mark	Marko, Peter	
Dragnea, Raluca	Marzsin, Thomas	

1.5 Fairness Monitor

1.5.1 To ensure the fairness, transparency and integrity of the procurement process, PWGSC has engaged a third-party Fairness Monitor for the entire process of this multi-phased procurement. The Fairness Monitor will not be part of the evaluation team, but will, among other things, observe the evaluation of the bid responses with respect to Canada's adherence to the evaluation process described in this RFP.

2 PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

2.1.1 All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the **Standard Acquisition Clauses and Conditions Manual** (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

2.1.2 Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

2.1.3 The 2003 (2015-07-03) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation, except that:

2.1.4 Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days
Insert: 365 day

2.1.5 The title of Section 10 is amended to read "Legal Capacity and Ownership and Control Information", the first paragraph is numbered as 1 and the following is added:

a. The Bidder must provide, if requested by the Contracting Authority, the following information as well as any other requested information related to the ownership and control of the Bidder, its owners, its management and any related corporations and partnerships:

b. An organizational chart for the Bidder showing all related corporations and partnerships;

c. A list of all the Bidder's shareholders and/or partners, as applicable; if the Bidder is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner; and

d. A list of all the Bidder's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the Bidder is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner.

e. In the case of a joint venture Bidder, this information must be provided for each member of the joint venture. The Contracting Authority may also require that this information be provided in respect of any subcontractors specified in a bid.

f. For the purposes of this section, a corporation or partnership will be considered related to another party if:

i. they are "related persons" or "affiliated persons" according to the *Canada Income Tax Act*;

ii. the entities have now or in the two years before the closing date had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

iii. the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

2.2 Submission of Bids

Bids must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation.

2.2.1 Due to the nature of the bid solicitation, bids transmitted by facsimile to PWGSC will not be accepted.

2.2.2 Write the PWGSC solicitation number and closing date on return envelope and on all separate pieces of the bid.

2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority, at the email address identified below, no later than 10 business days before the bid closing date. Enquiries received after that time may not be answered.

The Contracting Authority for the solicitation is:
Maxime Thauvette
Contracting Authority - EPS
Acquisitions Branch
PWGSC
Email: PANumerique.APDigital@tpsgc-pwgsc.gc.ca

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.4 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario, Canada.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or

territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.5 Improvement of Requirement during Solicitation Period

Should Bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, Bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favor a particular Bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled "Enquiries – Bid Solicitation". Canada will have the right to accept or reject any or all suggestions.

2.6 Volumetric Data

The volumetric data provided to Bidders in this solicitation document contains current and historical data. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of e-procurement services will be consistent with this data. It is provided purely for information purposes and will not form part of the resulting Contract. Bidders may decide in their sole discretion whether or not to take this information into consideration in preparation for their bids. Bidders may also decide in their sole discretion how to interpret and use this information during their bid preparation. Canada will not consider changes to a winning Bidder's proposal in the event that the actual volumetric data deviates from the one provided in this RFP. Canada will not be liable for any business loss the winning Bidder may claim during the performance of the contract due to fluctuations of the transaction volume.

2.7 Supply Chain Security Information (SCSI) Non-Disclosure Agreement

By submitting a bid, the Bidder agrees to the terms of the non-disclosure agreement below (the "**Non-Disclosure Agreement**"):

2.7.1 The Bidder agrees to keep confidential any information it receives from Canada regarding Canada's assessment of the Bidder's Supply Chain Security Information (the "**Sensitive Information**") including, but not limited to, which aspect of the Supply Chain Security Information is subject to concern, and the reasons for Canada's concerns.

2.7.2 Sensitive Information includes, but is not limited to, any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form or otherwise and whether or not that information is labeled as classified, proprietary or sensitive.

2.7.3 The Bidder agrees that it will not reproduce, copy, divulge, release or disclose, in whole or in part, in whatever way or form any Sensitive Information to any person other than a person employed by the Bidder who has a security clearance commensurate with the level of Sensitive Information being accessed, without the prior written consent of the Contracting Authority. The Bidder agrees

to immediately notify the Contracting Authority if any person, other than those permitted by this Article, accesses the Sensitive Information at any time.

2.7.4 All Sensitive Information will remain the property of Canada and must be returned to the Contracting Authority or destroyed, at the option of the Contracting Authority, if requested by the Contracting Authority, within 30 days following that request.

2.7.5 The Bidder agrees that a breach of this Non-Disclosure Agreement may result in disqualification of the Bidder at the RFP stage, or immediate termination of the resulting Contract. The Bidder also acknowledges that a breach of this Non-Disclosure Agreement may result in a review of the Bidder‘s security clearance and review of the Bidder‘s status as an eligible Bidder for other requirements.

2.7.6 This Non-Disclosure Agreement remains in force indefinitely.

3 PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

3.1.1 Canada requests that Bidders provide their bid in separately bound sections as follows:

a. Section I: Supply Chain Security Information (SCSI) (2 hard copies and 1 soft copy on a USB in a format accessible by Canada)

b. Section II: Technical Bid (1 hard copy and 1 soft copy on a USB in a format accessible by Canada) (can be on the same USB as Section I SCSI)

c. Section III: Financial Bid (1 hard copy and 1 soft copy on a USB in a format accessible by Canada)

d. Section IV: Certifications (1 hard copy and 1 soft copy on a USB (can be on the same USB as Section I SCSI and Section II Technical Bid)

e. If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy marked original will have priority over the wording of the soft copy.

f. Prices must appear in the financial bid only. Prices must not be indicated in any other section of the bid.

g. Formats of electronic documents accessible by Canada include PDF or MS Office 2013.

h. All electronic copies should include only one copy of the requested documents and be free of password protection.

3.1.2 In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Bidders should:

a. use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and

b. use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

c. include a table of contents; and

d. provide electronic copies in Microsoft Office 2013 or PDF

3.1.3 Bid Package

The Bidders are to ensure the structured bid package is provided as described above. Only referenced material included within the Bidder's response will be evaluated. Reference material outside of the Bidder's response will not be considered.

3.1.4 No Conditional Proposals

The Bidder must submit a bid for which it seeks to be considered as a Bidder. The Bidder's bid must not be made conditionally. Any condition imposed by the Bidder will render the bid non-responsive and the bid will be given no further consideration.

3.1.5 Submission of Only One Bid from a Bidder

a. The submission of more than one bid from a Bidder is not permitted in response to this bid solicitation. If a Bidder submits more than one bid, Canada will set aside all bids received from that Bidder.

3.1.6 Bidders additional Instructions:

a. Authorized Signature of Bidder:

Canada requires that each bid, at closing date and time or upon request from the Contracting Authority, be signed by the Bidder or by an authorized representative of the Bidder. If a bid is submitted by a joint venture, it must be done in accordance with Section 17 of the 2003 (2015-07-03) Standard Instructions – Goods or Services – Competitive Requirements which are incorporated by reference into and form part of the bid solicitation.

b. Cover Page:

The front cover page of each volume (or Section) of the bid should identify the title of the bid, the solicitation number, the volume number and the full legal name of the Bidder.

c. Table of Contents:

The page following the Cover Page of each volume of the bid should be the Table of Contents. The Table of Contents should contain a listing of all sections and subsections with associated page numbers. It should also list the associated tables, figures, and appendices contained in the part of the bid to which it refers.

d. Headers and Footers:

Each subsequent page of each volume of the bid should include a header and/or footer that includes the following information:

i. the bid title;
ii. the Bidder's name;
iii. the date of the bid; and

iv. the page number.

3.2 Section I: Supply Chain Security Information (SCSI)

3.2.1 Bidders must submit specific information regarding each component of their proposed e-Procurement Solution's supply chain. This information is referred to as *Supply Chain Security Information (SCSI)*. This information will be used by Canada to assess whether, in its opinion, a Bidder's proposed supply chain creates the possibility that the Bidder's proposed e-Procurement Solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with the Supply Chain Integrity Process identified in Part 4, section 4.3. This assessment is referred to as the SCSI Integrity Assessment.

3.2.2 The SCSI should include submission of Form 3 to Part 4 – SCSI - IT Product List and Subcontractor List Form, and any additional information required by the Contracting Authority to ensure a complete assessment; or must be provided upon request by the Contracting Authority within the timeframe identified in the request.

3.3 Section II: Technical Bid

3.3.1 In their Technical Bid, Bidders are requested to explain and demonstrate how their bid meets the RFP technical requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

3.3.2 It is requested that the Technical Bid include submission of Attachment 2 to Part 4 – Evaluation Criteria, Attachment 3 to Part 4 – Usability Assessment, Forms 1 to 3, and any other required documents as indicated elsewhere throughout this RFP; or must be provided upon request by the Contracting Authority within the timeframe identified in the request.

3.3.3 The Technical Bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

3.3.4 Bidders will not be permitted to modify any aspect of their Technical Bid as a result of any revised Supply Chain Security Information (SCSI) submitted.

3.3.5 Bidders will be provided with an electronic copy of some of the RFP documents, in Microsoft Office format, with the solicitation package issued on GETS. In the event of any discrepancies between the Microsoft Office copies and PDF documents released officially through GETS, the PDF documents released through GETS shall prevail.

3.4 Section III: Financial Bid

3.4.1 Bidders must submit their Financial Bid in accordance with Annex 3 – Price Schedule. The total amount of Applicable Taxes must be shown separately. Unless otherwise indicated, all prices must be firm prices.

3.4.2 Bidders Financial Bids must address each of the cost elements specified in this RFP. The Bidder must complete and submit Annex 3 – Price Schedule in an electronic and hard copy format to ensure consistency in the evaluation of each Bidder's Financial Bid. In the event of any discrepancies between the electronic and hard copy version of the Bidder's Financial Bid, the hard copy version shall prevail. The quoted prices shall be entered into the applicable cells of the Price Schedule only. Bidders must email the Contracting Authority, identified in section 2.3 Enquiries – Bid Solicitation, and request an electronic copy of the Price Schedule in Microsoft Excel format.

3.4.3 **All Costs to be included**: The Financial Bid must include all costs for the requirement described in the bid solicitation including any enhanced services identified in the Contractor's bid response, for the entire Contract Period including any option years. All necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.

3.4.4 Bidders will not be permitted to modify any aspect of their Financial Bid as a result of any revised Supply Chain Security Information (SCSI) submitted.

3.4.5 **Blank Prices:** Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, $0.00. No Bidder will be permitted to add or change a price as part of this confirmation. Any Bidder who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

3.4.6 SACC Manual Clause

The following clause, inserted by reference, forms part of this bid solicitation:
C3010T (2014-11-27), Exchange Rate Fluctuation Risk Mitigation

3.5 Section IV: Certifications

Bidders must submit the certifications required under Part 5.

3.6 Bidder's Proposed Site(s) or Premises Requiring Safeguarding Measures

3.6.1 As indicated in Part 6 under Security Requirements, the Bidder must provide the full address(es) of the Bidder's and proposed individual(s)' site(s) or premises for which safeguarding measures are required for Work Performance:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

3.6.2 The Company Security Officer (CSO) must ensure through the Industrial Security Program (ISP) that the Bidder and proposed individual(s) hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.

4 PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

Notice to Bidders: RFP Mandatory Evaluation Criteria are derived from, but not the same as, the mandatory evaluation criteria from the Invitation to Qualify (ITQ) taking into consideration feedback received during the Review and Refine Requirements (RRR) Process. All Bidders must respond to all RFP Mandatory Evaluation Criteria (see Attachment 2 to Part 4).

4.1 Evaluation Procedures

4.1.1 Bids will be assessed in accordance with the entire requirement of the bid solicitation. There are several steps in the evaluation process, which are described below. The evaluation and selection will be conducted in steps. The fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

4.1.2 An evaluation team composed of PWGSC and client department representatives will evaluate the bids on behalf of Canada. Canada may hire any independent consultant or use any Government resources to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

4.1.3 PWGSC has engaged a Fairness Monitor for this procurement. The Fairness Monitor will not be part of the evaluation team, but will observe the evaluation of the bids with respect to Canada's adherence to the evaluation process described in this bid solicitation.

4.1.4 In addition to any other time periods established in the bid solicitation:

a. **Requests for Clarifications**: If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

b. **Requests for Survey**: If Canada wishes to survey the Bidder's facilities, the Bidder should make its facilities available for this purpose within 10 working days of a request by the Contracting Authority. If the Bidder does not make its facilities available, the Bidder must be able to produce a certified 3rd party attestation, within 10 working days, that its facilities meet all requirements of this Solicitation.

c. **Extension of Time**: If additional time is required by the Bidder, the Contracting Authority may grant an extension at his or her sole discretion.

4.2 Technical Evaluation

4.2.1 Each bid will be reviewed in accordance with the evaluation process and method as described in Attachment 1 to Part 4 – Evaluation and Selection Methodology.

4.2.2 Each bid will be reviewed against the requirements and evaluation criteria as described in Attachment 2 to Part 4 – Evaluation Criteria and Attachment 3 to Part 4 – Usability Assessment, respectively.

4.2.3 In conducting its evaluation of the bids, Canada may, but will have no obligation to, do the following:

a. contact any or all references supplied by Bidders to verify and validate any information submitted by Bidders; and
b. seek clarification or verification from Bidders regarding any or all information provided by them with respect to the RFP.

4.2.4 Only referenced material included within the Bidder's bid, or clarified upon request by the Contracting Authority, will be evaluated. Reference material outside of the Bidder's bid will not be considered. It is the sole responsibility of the Bidder to provide sufficient information so that their bid can be adequately evaluated.

Note to Bidders: *In addition to any other obligations contained in the resulting contract, the winning Bidder will be contractually obliged to provide all services described in any of its responses to Attachment 2 to Part 4 – Evaluation Criteria, as well as any responses to Attachment 3 to Part 4 – Usability Assessment where it has been awarded technical points for such responses, in accordance with and at the prices contained in Annex 3 – Price Schedule. Canada will incorporate these obligations into the resulting contract Statement of Work. After contract award, the winning Bidder must deliver the required services in accordance with the Resulting Contract.*

4.3 Supply Chain Integrity Process

4.3.1 Definitions

The following words and expressions used in this Supply Chain Integrity process have the following meaning:

a. "Products" means any hardware that operates at the data link layer of the OSI Model (Layer 2) and above, any software and Workplace Technology Devices.

b. "Workplace Technology Devices" means desktops, mobile workstations such as laptops and tablets, smart phones, phones, and peripherals and accessories such as monitors, keyboards, computer mouse, audio devices and external and internal storage devices such as USB flash drives, memory cards, external hard drives and writable CD and DVD.

c. "Product Manufacturer" means the entity which assembles the component parts to manufacture a Product.

d. "Software Publisher: means the owner of the copyright of the software, who has the right to license (and authorize others to license/sub-license) its software products.

e. "Canada's Data" means any data originating from the Work, any data received in contribution to the Work or that is generated as a result of the delivery of security, configuration, operations, administration and management services, and any data that is transported or stored by the contractor or any subcontractor as a result of performing the Work.

f. "Work" means all the activities, services, goods, equipment, matters and things required to be done, delivered or performed by the Contractor under the resulting contract.

4.4 Mandatory Supply Chain Security Information (SCSI) Submission Requirements

4.4.1 Attachment 4 to Part 4 – Supply Chain Scope Diagram provides a visual representation of the SCSI requirement which the Bidders, must provide.

4.4.2 Bidders must submit, with their bid, the following SCSI:

a. **IT Product List**: Bidders must identify the Products over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work described in the resulting contract, as well as the following in regards to each Product:

b. Location: identify where the Product is interconnected within any given network for Canada's Data (identify the service delivery points or nodes, such as points of presence, third party locations, data centre facilities, operations center, security operations center, internet or other public network peering points, etc.);

c. Product Type: identify the generally recognized description used by Industry such as appliance, hardware, software, etc. Components of an assembled Product, such as a module or card assembly, must be provided for all layer 3 internetworking devices;

d. IT Component: identify the generally recognized description used by Industry such as firewall router, switch, server, security appliance, etc.;

e. Product Model Name or Number: identify the advertised name or number of the Product by the Product Manufacturer;

f. Description and Purpose of the Product: identify the advertised description or purpose by the Product Manufacturer of the Product and the intended usage or role in the Work described in the resulting contract;

g. Identify the Product Manufacturer and/or Software Publisher;

h. Name of Subcontractor refers to the subcontractor that will provide the Product.

i. Bidders are requested to provide the IT Product List information on Form 3 to Part 4 – SCSI - IT Product List and Subcontractor List Form. It is requested that the Bidders indicate their legal name on each page and insert a page number as well as the total number of pages. Bidders are also requested to insert a separate row for each Product. Bidders are requested not to repeat multiple iterations of the same Product (e.g. if the serial number

and/or the color is the only difference between two Products, they are considered the same Product with regards to SCSI).

4.4.3 **Network Diagrams**: one or more conceptual network diagrams that collectively show the complete network proposed to be used to deliver the services described in the Statement of Work. The network diagrams are only required to include portions of the Bidder's network (and its subcontractor' network(s)) over which Canada's Data, would be transmitted in performing any resulting contract. As a minimum the diagram must show:

a. The following key nodes for the delivery of the services under the resulting contract of this solicitation process, if applicable the role of the Bidder or subcontractor;
   i. Service delivery points;
   ii. Core network
   iii. Subcontractor network (specifying the name of the subcontractor as listed in the List of Subcontractors);
   iv. The node interconnections, if applicable
   v. Any node connections with the Internet; and
   vi. For each node, a cross-reference to the product that will be deployed within that node, using the line item number from the IT Product List.

4.4.4 **List of Subcontractors**: The Bidder must provide a list of any subcontractors that could be used to perform any part of the Work (including subcontractors affiliated or otherwise related to the Bidder) pursuant to any resulting contract. The list must include at a minimum:

a. The name of the subcontractor;
b. The address of the subcontractor's headquarters;
c. The portion of the Work that would be performed by the subcontractor; and
d. The location(s) where the subcontractor would perform the Work.
e. This list must identify all third parties who may perform any part of the Work, whether they would be subcontractors to the Bidder, or subcontractors to subcontractors of the Bidder down the chain. Any subcontractor that could have access to Canada's Data must be identified. For the purposes of this requirement, a third party who is merely a supplier of goods to the Bidder, but who does not perform any portion of the Work, is not considered to be a subcontractor. Subcontractors would include, for example, technicians who might be deployed or maintain the Bidder's solution. If the Bidder does not plan to use any subcontractors to perform any part of the Work, the Bidder is requested to indicate this in its response.
f. Bidders are requested to provide their information on Form 3 to Part 4 – SCSI - IT Product List and Subcontractor List Form. It is requested that Bidders indicate their legal name on each page, insert a page number as well as the total number of pages. Bidders are also requested to insert a separate row for each subcontractor and additional rows as may be necessary.

4.5 Assessment of Supply Chain Security Information

4.5.1 In conducting its assessment:

a. Canada may request from the Bidder any additional information that Canada requires to conduct a complete security assessment of the Supply Chain Security Information. The Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being deemed non-responsive.
b. Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the response or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the Supply Chain Security Information.

4.5.2 If, in Canada's opinion, any aspect of the Supply Chain Security Information, if used in a solution, creates the possibility that the Bidder's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

a. Canada will notify the Bidder in writing (sent by email) and identify which aspect(s) of the Supply Chain Security Information is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Bidder regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Bidder; therefore, in some circumstances, the Bidder will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the Bidder's Supply Chain Security Information.
b. The notice will provide the Bidder with one opportunity to submit revised Supply Chain Security Information within the 10 calendar days following the day on which Canada's written notification is sent to the Bidder, (or a longer period specified in writing by the Contracting Authority).
c. Bidders will not be permitted to modify any aspect of their Technical Bid or Financial Bid as a result of any revised SCSI submitted.
d. If the Bidder submits revised Supply Chain Security Information within the allotted time, Canada will perform a second assessment. If Canada determines that any aspect of the Bidder's revised Supply Chain Security Information could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, no further opportunities to revise the Supply Chain Security Information will be provided and the bid will be deemed non-responsive.

4.5.3 By participating in this process, the Bidder acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. Also, the Bidder acknowledges that Canada's security assessment does not involve the assessment of a proposed solution.

As a result:

a. at any time during the subsequent stages of this bid solicitation process, Canada may advise a Bidder that some aspect(s) of its Supply Chain Security Information has become the subject of security concerns. At that point, Canada will notify the Respondent and provide the Bidder with an opportunity to revise its Supply Chain Security Information, using the same process described above.

b. during the performance of a subsequent contract, if Canada has concerns regarding certain products, designs or subcontractors originally included in the Supply Chain Security Information, the terms and conditions of that contract will govern the process for addressing those concerns.

4.5.4 All Bidders will be notified in writing regarding whether or not they pass the SCI checks.

4.5.5 Once a Bidder has passed the SCI checks during the RFP evaluations, no modifications are permitted to the Supply Chain Security Information except under exceptional circumstances, as determined by Canada. Given that not all the exceptional circumstances can be foreseen, whether changes may be made and the process governing those changes will be determined by Canada on a case-by-case basis.

4.6 Financial Evaluation

4.6.1 The Financial Evaluation will be conducted in accordance with the evaluation process and method as described in Attachment 1 to Part 4 – Evaluation and Selection Methodology and the following SACC Manual Clause:

SACC Manual Clause A0220T (2014-06-26), Evaluation of Price.

4.6.2 Formulae in Pricing Tables

Where the pricing tables provided to Bidders include any formulae, Canada may re-input the prices provided by Bidders into a fresh table if Canada believes that the formulae may no longer be functioning properly in the version submitted by a Bidder.

4.6.3 Substantiation of Professional Services Rates

In Canada's experience, Bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates for professional services bid, Canada may, but will have no obligation to, require price support for any rates proposed (either for all or for a specific Resource Category). If Canada requests price support, it will be requested from all responsive Bidders proposing a rate that is at least 20% lower than the median rate bid by all

responsive Bidders for the relevant Resource Category or Categories. Where Canada requests price support, the following information is required:

a. an invoice (referencing a contract serial number) that shows that the Bidder has recently provided and invoiced another customer (with whom the Bidder deals at arm's length) for services performed for that customer similar to the services that would be provided in the relevant Resource Category, where those services were provided in the National Capital Region for at least three months within the twelve months prior to the bid solicitation issuance date, and the fees charged were equal to or less than the rate offered to Canada;

b. in relation to the invoice in (i), a signed contract with, or a letter of reference signed by, the Bidder's client that includes at least 50% of the tasks listed in this solicitation's Statement of Work for the Resource Category being examined for an unreasonably low rate;

c. in respect of each referenced contract, a resume for the resource that performed under that contract that shows the resource would pass the Resource Category's mandatory requirements and achieve the required pass mark for the Resource Category's rated criteria; and

d. the name, telephone number and, if available, e-mail address of the invoiced client for each of the resources invoiced, so Canada can verify any facts presented for the affected categories.

4.6.4 Once Canada requests substantiation of the rates bid for any Resource Category, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada) that will allow Canada to determine whether it can rely, with confidence, on the Bidder's ability to provide the required services at the rates bid. Where Canada determines that the information provided by the Bidder does not substantiate the unreasonably low rates, the proposal will be considered non-responsive and will receive no further consideration. Only the Firm Per Diem Rates of bids that are technically responsive will be considered.

4.7 Reference Checks

4.7.1 The Bidder is requested to provide a third-party reference for each project in its bid as requested in Attachment 1 to Part 4 – Evaluation Criteria, using Form 2 – Project Reference Check Form. If information requested is not provided in the bid, the Bidder must provide the information upon request by the Contracting Authority within the timeframe identified in the request. References from representatives of Canada will be accepted.

4.7.2 It is the responsibility of the Bidder to confirm in advance that their client contact for the project reference will be available to provide a response and is willing to provide a reference.

4.7.3 For the purpose of this evaluation, reference checks may be used to verify and validate the Bidder’s bid response. If a reference check is performed, Canada will conduct the reference check in writing by e-mail. Canada will send the reference check request directly to the client contact for the project reference provided by the Bidder. The client contact will have 10 working days (or a longer period otherwise specified in writing by the Contracting Authority) from the date that Canada's e-mail was sent, to respond to Canada.

4.7.4 The client contact will be required, within 2 working days after Canada sends out the reference check request, to acknowledge the receipt of the reference check request and indentify his or her willingness and availability to conduct such reference check. If Canada has not received the required response from the client contact, Canada will notify the Bidder by e-mail, to allow the Bidder to contact its client contact directly to ensure that he or she responds to Canada within the allotted time. The client contact's failure to timely respond to Canada's request will result in non-consideration of the Bidder's claimed project experience.

4.7.5 Notwithstanding section 4.7.4, if the client contact is unavailable when required during the evaluation period, the Bidder will be requested to provide an alternate client contact for the same referenced project. Bidders will only be provided with this opportunity once for each referenced project and only if the original client contact is unavailable to respond. The process as described in 4.7.4 is applicable for the reference check with the alternate client contact. The period to respond for either the original client contact, or the alternate client contact, will be a total of 10 working days (or a longer period otherwise specified in writing by the Contracting Authority) in accordance with 4.7.4.

4.7.6 Wherever information provided by a client contact differs from the information supplied by the Bidder, the Bidder will be asked to clarify project reference information provided in its bid response. Canada will assess the following information during the evaluation of the Bidder's bid response: the Bidder's original project reference information; any information provided by the Bidder in response to clarification request(s); and any information supplied by the client contact for the referenced project.

4.7.7 A Bidder will not pass the Reference Check if:

a. the client contact fails to timely respond to Canada's request;

b. the client contact states he or she is unable or unwilling to provide the information requested;

c. the information provided by the Bidder cannot be verified and validated by Canada; or

d. the client contact organization and/or client contact has ever been or is currently affiliated with the Bidder; or if the client contact organization is an entity that does not deal at arm's length with the Bidder.

4.7.8 A Bidder who has failed in any Reference Check, as a result of 4.7.7, for the Mandatory Requirements (Attachment 2 to Part 4) will be deemed not fully meeting the mandatory requirements.

4.7.9 A Bidder who has failed in any Reference Check, as a result of 4.7.7, for the Rated Requirements (Attachment 2 to Part 4) will not be awarded with the points associated with the respective rated criterion that requests the reference check.

4.8 Basis of Selection

4.8.1 To be declared responsive, a bid must:

a. Comply with all the requirements for the bid solicitation;

b. Pass the Supply Chain Security Assessment;

c. Meet all the mandatory requirements outlined in the Mandatory Requirements (Attachment 2 to Part 4); and

d. Obtain minimum pass mark(s) for Rated Requirements (Attachment 2 to Part 4).

4.8.2 Canada will determine the top-ranked bid in accordance with the selection method as described in Attachment 1 to Part 4 – Evaluation and Selection Methodology.

4.8.3 Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

5 PART 5 - CERTIFICATIONS

Bidders must provide the required certifications and associated information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Canada will declare a bid non-responsive, or will declare a contractor in default in carrying out any of its obligations under the Contract, if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority may render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Precedent to Contract Award

The certifications listed below should be completed and submitted with the bid but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to comply with the request of the Contracting Authority and to provide the certifications within the time frame specified will render the bid non-responsive.

5.2 Integrity Provisions - Associated Information

5.2.1 By submitting a bid, the Bidder certifies that the Bidder and its Affiliates are in compliance with the provisions as stated in Section 01 Integrity Provisions - Bid of Standard Instructions 2003 (2015-07-03). The associated information required within the Integrity Provisions will assist Canada in confirming that the certifications are true.

5.2.2 Pursuant to the Integrity Provisions under section 01 of Standard Instructions 2003, Bidders must provide a list of all owners and/or Directors and other associated information as required. Refer to section 4.21 of the Supply Manual for additional information on the Integrity Provisions.

5.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, Bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

5.4 Definitions

For the purposes of this clause, “former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police.

A former public servant may be:

a. an individual;
b. an individual who has incorporated;
c. a partnership made of former public servants; or
d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

5.5 Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

a. name of former public servant;
b. date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder’s status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

5.6 Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information:

a. name of former public servant;
b. conditions of the lump sum payment incentive;
c. date of termination of employment;
d. amount of lump sum payment;
e. rate of pay on which lump sum payment is based;
f. period of lump sum payment including start date, end date and number of weeks;
g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes."

5.7 Federal Contractors Program for Employment Equity - Bid Certification

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list (http://www.labour.gc.ca/eng/standards_equity/eq/emp/fcp/list/inelig.shtml) available from Employment and Social Development Canada (ESDC) - Labour's website.

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid " list at the time of contract award.

Canada will also have the right to terminate the contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

5.8 Bid-Certification

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) – Labour's website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the *Employment Equity Act*.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).

( ) A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)

5.9 Status and Availability of Resources

The Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives. If for reasons beyond its control, the Bidder is unable to provide the services of an individual named in its bid, the Bidder may propose a substitute with similar qualifications and experience. The Bidder must advise the Contracting Authority of the reason for the substitution and

provide the name, qualifications and experience of the proposed replacement. For the purposes of this clause, only the following reasons will be considered as beyond the control of the Bidder: death, sickness, maternity and parental leave, retirement, resignation, dismissal for cause or termination of an agreement for default.

If the Bidder has proposed any individual who is not an employee of the Bidder, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

5.10 Education and Experience

The Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

5.11 Acknowledgement

By submitting a bid, the Bidder represents that it has full authority to bind the company to all the terms and conditions contained herein.

6 PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements

a. At the date of bid closing, the following conditions must be met:

For Canadian Suppliers

i. Canadian Bidders must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses, 7.5 A.,a. Security Requirement for Canadian Suppliers.

ii. Canadian Bidders' proposed individuals requiring access to **PROTECTED** information, assets or sensitive work site(s) or to privileged access to IT Systems must meet the security requirement as indicated in Part 7 - Resulting Contract Clauses, 7.5 A.,b. Security Requirement for Canadian Suppliers.

iii. The Bidder must provide the address(es) of proposed site(s) or premises of work performance and document safeguarding as indicated in Part 3 - section 3.6 Bidder's Proposed Site(s) or Premises Requiring Safeguarding Measures.

iv. Bidders are reminded to obtain the required security clearance promptly as the Work must not be started without the requisite security clearances. Any delay in the award of the contract to allow the successful bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

v. For additional information on security requirements, Bidders should refer to the Industrial Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

For Foreign Suppliers

i. International Bidders must be from a country that has an international bilateral industrial security instrument with the Industrial Security Program (ISP) of PWGSC as indicated in Part 7 – Resulting Contract Clauses, 7.5 B.,a. The ISP has international bilateral industrial security instruments with the countries listed on the following PWGSC website: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-eng.html.

ii. The Bidder must provide the address(es) of proposed site(s) or premises of work performance and document safeguarding as indicated in Part 3 - section 3.6 Bidder's Proposed Site(s) or Premises Requiring Safeguarding Measures.

iii. The Bidders must provide proof that they are incorporated or authorized to do business in their jurisdiction as indicated in Part 7 - Resulting Contract Clauses, 7.5 B.,c. Security Requirement for Foreign Suppliers.

iv. The Bidders must be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country (ies) in which it is incorporated or authorized to do business and operating as indicated in

Part 7 - Resulting Contract Clauses, 7.5 B.,b. Security Requirement for Foreign Suppliers.

v. The Bidders must provide the names of all individuals who will require access to Personal Information, assets or sensitive work site(s) or to privileged access to IT Systems and must meet the security requirement as indicated in Part 7 - Resulting Contract Clauses, 7.5 B.,f.,g Security Requirement for International Suppliers.

vi. Bidders are reminded to obtain the required security clearance promptly as the Work must not be started without the requisite security clearances. Any delay in the award of the contract to allow the successful bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

vii. For additional information on security requirements, Bidders should refer to the Industrial Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

viii. In the case of a joint venture Bidder, each member of the joint venture must meet the security requirements.

6.2 Financial Capability

The following clause, inserted by reference, forms part of this bid solicitation:

SACC Manual clause A9033T (2012-07-16) Financial Capability

7 PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Requirement

7.1.1 _____ (the "**Contractor**") agrees to supply to the Client the services described in the Contract, including all the Annexes, in accordance with, and at the prices set out in the Contract.

7.1.2 **Client:** Any reference to "Client" or "Clients" includes any Canadian government department, Crown corporation or agency as described in the *Financial Administration Act* (as amended from time to time); any other party for which the Department of Public Works and Government Services has been authorized to act from time to time under section 16 of the *Department of Public Works and Government Services Act; and any suppliers using the contracted solution.*

7.1.3 **Reorganization of Client**: The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Project Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

7.1.4 **Defined Terms**: Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions.

7.2 Supply Chain Integrity Process Definitions

The following words and expressions used in this Supply Chain Integrity Process have the following meaning:

a. "Products" means any hardware that operates at the data link layer of the OSI Model (Layer 2) and above, any software and Workplace Technology Devices.

b. "Workplace Technology Devices" means desktops, mobile workstations such as laptops and tablets, smart phones, phones, and peripherals and accessories such as monitors, keyboards, computer mouse, audio devices and external and internal storage devices such as USB flash drives, memory cards, external hard drives and writable CD and DVD.

c. "Product Manufacturer" means the entity which assembles the component parts to manufacture a Product.

d. "Software Publisher: means the owner of the copyright of the software, who has the right to license (and authorize others to license/sub-license) its software products.

e. “Canada’s Data” means any data originating from the Work, any data received in contribution to the Work or that is generated as a result of the delivery of security, configuration, operations, administration and management services, and any data that is transported or stored by the Contractor or any subcontractor as a result of performing the Work.

f. "Work" means all the activities, services, goods, equipment, matters and things required to be done, delivered or performed by the Contractor under the resulting Contract.

7.3 Task Authorization

The Work or a portion of the Work to be performed under the Contract will be on an "as and when requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract.

7.3.1 Task Authorization Process:

a. The Project Authority will provide the Contractor with a description of the task using the form specified in Annex 7 – Task Authorization Form.
b. The Task Authorization (TA) will contain the details of the activities to be performed, a description of the deliverables, and a schedule indicating completion dates for the major activities or submission dates for the deliverables. The TA will also include the applicable basis (bases) and methods of payment as specified in the Contract.
c. The Contractor must provide the Project Authority, within 5 calendar days of its receipt, or a timeframe as agreed with the Project Authority, the proposed total estimated cost for performing the task and a breakdown of that cost, established in accordance with the Price Schedule specified in Annex 3 of the Contract.
d. The Contractor must not commence work until a TA authorized by the Project Authority has been received by the Contractor. The Contractor acknowledges that any work performed before a TA has been received will be done at the Contractor's own risk.

7.3.2 Task Authorization Limit

a. The Project Authority may authorize individual Task Authorizations up to a limit of $100,000.00 (excluding GST/HST), inclusive of any revisions.

b. Any Task Authorization to be issued in excess of that limit must be authorized by the Contracting Authority before issuance.

7.3.3 Consolidation of Task Authorizations for Administrative Purposes

The Contract may be amended by the Contracting Authority from time to time to reflect all TAs issued and approved to date, to document the Work performed under those TAs for administrative purposes.

7.3.4 Canada's Obligation - Portion of the Work - Task Authorizations

a. Canada’s obligation with respect to the portion of the Work under the Contract that is performed through Task Authorizations is limited to the total amount of the actual tasks performed by the Contractor.

b. Canada reserves the right, at any time, to compete any Tasks and to select other suppliers. This includes the right to compete any task for which the Contractor provided a written proposal that has been rejected by Canada.

7.3.5 Periodic Usage Reports - Contracts with Task Authorizations

a. The Contractor must compile and maintain records on its provision of services to the federal government under authorized Task Authorizations issued under the Contract.

b. The Contractor must provide this data in accordance with the reporting requirements detailed below. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "nil" report.

c. The data must be submitted on a quarterly basis to the Contracting Authority.

The quarterly periods are defined as follows:
1st quarter: April 1 to June 30;
2nd quarter: July 1 to September 30;
3rd quarter: October 1 to December 31; and
4th quarter: January 1 to March 31.

d. The data must be submitted to the Contracting Authority no later than 5 calendar days after the end of the reporting period.

7.3.6 Reporting Requirement- Details

A detailed and current record of all authorized tasks must be kept for the Contract. This record must contain:

a. the authorized task number or task revision number(s);
b. a title or a brief description of each authorized task;
c. the total estimated cost specified in the authorized Task Authorization (TA) of each task, exclusive of Applicable Taxes;
d. the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;
e. the start and completion date for each authorized task;
f. the active status of each authorized task, as applicable;
g. the amount (exclusive of Applicable Taxes) specified in the contract (as last amended, as applicable) as Canada's total liability to the contractor for all authorized TAs; and
h. the total amount, exclusive of Applicable Taxes, expended to date against all authorized TAs.

7.4 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

7.4.1 General Conditions

a. 2035 (2015-07-03), General Conditions – Higher Complexity - Services, apply to and form part of the Contract.

b. The 2035 General Conditions – Higher Complexity Services, are amended as follows:

(i) Delete subsection entitled “Replacement of Specific Individuals” in its entirety.
(ii) Insert subsection entitled “Replacement of Specific Individuals” with the following content:

1. If the Contractor is unable to provide the services of any specific individual identified in the Contract to perform the services, the Contractor must within five working days of the individual's departure or failure to commence Work (or, if Canada has requested the replacement, within ten working days of Canada's notice of the requirement for a replacement) provide to the Contracting Authority:

   a. the name, qualifications and experience of a proposed replacement immediately available for Work; and
   b. security information on the proposed replacement as specified by Canada, if applicable.
   c. The replacement must have qualifications and experience that meet or exceed those obtained for the original resource.

2. Subject to an Excusable Delay, where Canada becomes aware that a specific individual identified under the Contract to provide services has not been provided or is not performing, the Contracting Authority may elect to:

   a. exercise Canada's rights or remedies under the Contract or at law, including terminating the Contract for default under Section titled "Default of the Contractor", or
   b. assess the information provided under 1.c. above or, if it has not yet been provided, require the Contractor propose a replacement to be rated by the Project Authority. The replacement must have qualifications and experience that meet or exceed those obtained for the original resource and be acceptable to Canada.
   c. Upon assessment of the replacement, Canada may accept the replacement, exercise the rights in 2.a. above, or require another replacement in accordance with this sub-article c.

3. Where an Excusable Delay applies, Canada may require 2.b. above instead of terminating under the "Excusable Delay" Section. An Excusable Delay does not include resource unavailability due to allocation of the resource to another Contract or project (including those for the Crown) being performed by the Contractor or any of its affiliates. The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that a resource stop performing the Work. In such a case, the Contractor must immediately comply with the order. The fact that the Contracting Authority does not order that a resource stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.

4. The obligations in this article apply despite any changes that Canada may have made to the Client's operating environment.

7.4.2 Supplemental General Conditions

The following Supplemental General Conditions apply to and form part of the Contract.

a. 4006 (2010-08-16), Supplemental General Conditions – Contractor to Own Intellectual Property Rights in Foreground Information; and

b. 4008 (2008-12-12), Supplemental General Conditions – Personal Information.

7.5 Security Requirements

The following security requirements apply and form part of the Contract.

A. SECURITY REQUIREMENTS FOR CANADIAN SUPPLIERS:

These security clauses apply to the Contractor and/or any and all subcontractors delivering the services (referred to in Annex 2 - Security and Privacy) and performing the Work listed and described in Annex 1 – Statement of Work. These security requirements are in addition to those requirements already identified in Part 7 - Resulting Contract Clauses, section 7.5.2 Protection and Security of Data Stored in Databases For Canadian and Foreign Suppliers, section 7.5.3 - Privacy and Personal Information, and Annex 2 - Security and Privacy. Should any changes occur during the performance of the Contract, or at the request of the Contracting Authority, the Contractor must provide an updated completed Annex 2 - Security and Privacy.

a. The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level of **SECRET**, with approved Document Safeguarding at the level of **PROTECTED B**, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

b. The Contractor personnel requiring access to **PROTECTED** information, assets or sensitive work site(s) must **EACH** hold a valid personnel security screening at the level of **SECRET**, or **RELIABILITY STATUS, as required** granted or approved by the CISD, PWGSC.

c. Until the security screening of the Contractor personnel required by this Contract has been completed satisfactorily by the Canadian Industrial Security Directorate, Public Works and Government Services Canada, the **Contractor** personnel **MAY NOT HAVE ACCESS to PROTECTED** information or assets, and **MAY NOT ENTER** sites where such information or assets are kept, without an escort.

d. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store any sensitive **PROTECTED** information until CISD/PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of **PROTECTED B.**

e. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of CISD/PWGSC.

f. The Contractor must comply with the provisions of the:

   i. Security Requirements Check List and security guide attached at Annex 4.

   ii. Industrial Security Manual (Latest Edition) http://ssi-iss.tpsgc-pwgsc.gc.ca/msi-ism/index-eng.html

g. The Contractor and/or any and all subcontractors must NOT share or disclose PROTECTED information or data with any entity in Canada that does not conform with applicable privacy legislation (provincial or federal as the case may be) and industry standards.

h. The Contractor and/or any and all subcontractors must NOT share or disclose PROTECTED information or data with an entity outside of Canada that does not conform with the applicable privacy legislationof the country in which it is domiciled and industry standards.

i. Canada has the right to reject any request to electronically access, process, produce, transmit or store Personal Information related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

j. Any and/or all foreign subcontractors must immediately report to its respective national DPA and the Contracting Authority and Project Authority (in collaboration with the Canadian DSA) all cases in which it is known or there is reason to suspect that any Personal Information provided or generated pursuant to this Contract and/or subcontract have been lost, or in contravention of these security requirements, used or disclosed.

k. Any and/or all foreign subcontractors must contact their national DPA for further information regarding the safeguarding, management, cross-border transfer and protection of personal data.

l. Any and/or all foreign subcontractors must ensure that the appropriate security clauses, as determined by the Canadian DSA, are inserted in all subcontracts that involve access to Personal Information provided to or generated under this Contract and/or

subcontract and must ensure that the conditions placed on a subcontractor are no less favourable to Canada than the conditions set out in these security requirements.

m. Any/and or all foreign subcontractors visiting Canadian Government, under this contract, will submit a Request for Visit form to the Departmental Security Officer of Public Works and Government Services Canada. Further information on the responsibilities of a CSO and instructions on completing the form can be found at: http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html

n. Upon first time visit to Canadian Government or industrial sites, any and/or all foreign subcontractors must bring proof of a police record check (criminal record check) or recognized equivalent to be provided at time of visit.

B. SECURITY REQUIREMENTS FOR FOREIGN SUPPLIERS:

The Canadian Designated Security Authority (Canadian DSA) for industrial matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming Contractor and/or subcontractor compliance with the security requirements for foreign suppliers. The following security clauses apply to the Contractor and/or any and all subcontractors incorporated or authorized to do business in a jurisdiction other than Canada and delivering outside Canada the goods listed and described in Annex 1 – Statement of Work of the Contract. These security requirements are in addition to those requirements already identified in Part 7 – Resulting Contract Clauses, section 7.5.2 Protection and Security of Data Stored in Databases For Canadian and Foreign Suppliers, and section 7.5.3 - Privacy and Personal Information. Notwithstanding the provisions of SACC 2035 (06), in the event the Contractor seeks to subcontract respecting the Work, such subcontracts are not to be awarded or used without the prior written consent of the Canadian DSA and must meet the following terms.

a. The Contractor must be from a Country with which Canada has an international bilateral industrial security instrument. The Industrial Security Program (ISP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-eng.html

b. The Contractor and/or any and all subcontractors must at all times during the performance of the Contract be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or is operating and authorized to do business.

c. The Contractor and/or any and all subcontractors must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and identify the relevant national Privacy Authority. For European Contractors, this will be the national Data Protection Authority (DPA);

d. The Contractor and/or any and all subcontractors must comply with the provisions of the Security Requirements Check List, attached at Annex 4.

e. Any and/or all Canadian subcontractors must at all times during the performance of the Contract and/or subcontract, hold a valid Designated Organization Screening (DOS) at the level of PROTECTED B, issued by CISD/PWGSC.

f. The foreign Contractor shall not permit access to Canadian restricted sites or grant access to **CANADA PROTECTED** information, except to its personnel subject to the following conditions:

   i. Personnel have a need-to-know for the performance of the Contract;

   ii. Personnel have been subject to a criminal record check, with favourable results, from a recognized Governmental agency in their country as well as a background verification. The approved verifications for the required criminal record check and background verification are listed at 7.5.1 below these clauses.

   iii. The Foreign Contractor will ensure that its Chief Executive Officer (CEO) or Senior Official of the company will appoint a Contract Security Officer (CSO) and/or an Alternate Contract Security Officer (ACSO) in order to ensure compliance with all contracting security requirements.

   iv. The Foreign Contractor shall ensure that personnel provide consent to share results of the Criminal record Background Check with the Canadian DSA and other Canadian Government Officials, if requested;

   v. The Government of Canada reserves the right to deny access to **Canadian PROTECTED** information and/ or assets to a Foreign Recipient Contractor for cause.

g. In accordance with the Security Classification Guide, the following Canadian or Foreign Contractor personnel requiring privileged access to Information Technology systems shall each hold a valid Personnel Security clearance at the **SECRET** level granted by their respective NSA/DSA, in accordance with the National Policies of their country:

   i. Any e-Procurement Solution (EPS) Contractor personnel with physical access to the EPS infrastructure at Contract Service Delivery Points (SDP), includes Contractor data centers, Security Operations Center (SOC), Network Operations Center (NOC).

   ii. Contractor Security Operations Center (SOC) Personnel

iii. Contractor Operations Center Personnel

h. The Contractor and/or any and all subcontractors must at all times protect the privacy of any Personal Information, as defined in Part 7 – Resulting Contract Clauses, section 7.5.2 – Privacy and Personal Information, and as understood in Canadian Law, specifically the *Privacy Act* (1985) and the *Personal Information Protection and Electronic Documents Act* (2000) and must, at a minimum, restrict access to the Personal Information to Contractor personnel who:

i. Have successfully passed a criminal records check during the employment screening process with that organization; and

ii. Have demonstrated a "need-to-know" and require access to the Personal Information to perform the Contract.

i. The Contractor and/or any and all subcontractors acknowledges and agrees that its obligations to safeguard, manage, and protect all Personal Information under the Contract are in addition to any obligations it has under national privacy legislation of the country(ies) in which it is incorporated or operates.

j. All Personal Information, provided to the Contractor and/or any and all subcontractors or produced by the Contractor and/or any and all subcontractors, must:

i. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the Contract, without the prior written consent of the Government of Canada. Such consent must be sought from its national DPA and the Contracting Authority (in collaboration with the Canadian DSA).

ii. not be used for any purpose other than for the performance of the Contract without the prior written approval of the Government of Canada. This approval must be obtained by contacting its national DPA and the Contracting Authority (in collaboration with the Canadian DSA).

k. The Contractor and/or any and all subcontractors must immediately report to its respective national DPA and the Contracting Authority (in collaboration with the Canadian DSA) all cases in which it is known or there is reason to suspect that any Personal Information provided or generated pursuant to this Contract and/or subcontract have been lost, or in contravention of these security requirements, used or disclosed.

l. The Contractor and/or any and all subcontractors must contact their national DPA for further information regarding the safeguarding, management, cross-border transfer and protection of personal data.

m. The Contractor and/or any and all subcontractors must ensure that the appropriate security clauses, as determined by the Canadian DSA, are inserted in all subcontracts that involve access to Personal Information provided to or generated under this Contract

and/or subcontract and must ensure that the conditions placed on a subcontractor are no less favourable to Canada than the conditions set out in these security requirements.

n. Canada has the right to reject any request to electronically access, process, produce, transmit or store Personal Information related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

o. The Contractor visiting Canadian Government, under this contract, will submit a Request for Visit form to the Departmental Security Officer of Public Works and Government Services Canada.

7.5.1 The Foreign Contractor must perform a security screening of all its personnel who will need access to **CANADA PROTECTED** information and/or to Canadian restricted sites:

a. Identity check
   i. Copies of two of valid original pieces of government issued identity documentation, one of which must include a photo
   ii. Surname (last name)
   iii. Full given names (first name) – underline or circle usual name used
   iv. Family name at birth
   v. All other names used (aliases)
   vi. Name changes
      1. Must include the name they changed from and the name they changed to, the place of change and the institution changed through
   vii. Sex
   viii. Date of birth
   ix. Place of birth (city, province/state/region, and country)
   x. Citizenship(s)
   xi. Marital status/common-law partnership
      1. Current Status (married, common-law, separated, widowed, divorced, single)
      2. All current spouses (if applicable)
         a. Surname (last name)
         b. Full given names (first name) – underline or circle usual name used
         c. Date and duration of marriage/common-law partnership
         d. Date of birth
         e. Family name at birth
         f. Place of birth (city, province/state/region, and country)
         g. Citizenship

b. Residency check
   i. The last five (5) years of residency history starting from most recent with no gaps in time.
      1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates

c. Educational check
    i. The educational establishments attended and the corresponding dates.

d. Employment history check
    i. The last five (5) years of employment history starting from most recent with no gaps in time.
    ii. Three (3) employment reference checks from the last five (5) years.

e. Criminal records check:
    i. report(s) containing all criminal convictions for the last five (5) years in and outside of the candidate's country of residence.

7.5.2 Protection and Security of Data Stored in Databases for Canadian and Foreign Suppliers:

a. The Contractor and/or any and all subcontractors must ensure that all the databases used by organizations to provide the services described in Annex 1 – Statement of Work containing any Personal Information, related to the Work, are located in Canada or in the following additional countries with which Canada has a Bilateral and Multinational Memorandum of Understanding and Industrial Security Arrangement: Australia, Belgium, Denmark, Finland, France, Germany, Israel, Italy, Netherlands, New Zealand, Norway, Spain, Sweden, Switzerland, The United Kingdom, The United States.

b. The Contractor and/or any and all subcontractors must control access to all databases, referred to in subsection a, on which any Personal Information related to the Work is stored so that only individuals with the appropriate security clearance are able to access the database, either by using a password or other form of access control.

c. The Contractor must ensure that all databases on which any data relating to the Contract is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases, unless those databases are located in Canada (or in another country approved by the Contracting Authority ((in collaboration with the Canadian DSA) under subsection a and otherwise meet the requirements of this article.

d. The Contractor must ensure that all data relating to the Contract is processed only in Canada or in another country approved by the Contracting Authority and Project Authority (in collaboration with the Canadian DSA) under subsection a.

e. Despite any section of the General Conditions relating to subcontracting, the Contractor and/or any and all subcontractors must not subcontract (including to a parent, subsidiary or affiliate) any function, relating to the provision of services described in Annex 1 – Statement of Work, that involves providing a subcontractor with access to any Personal Information related to the Work unless the Contracting Authority and

Project Authority (in collaboration with the Canadian DSA) first consents in writing.

7.5.3 Privacy and Personal Information

a. Interpretation

i. In the Contract, unless the context otherwise requires,

"General Conditions" means the general conditions that form part of the Contract

"Personal Information" means information about an individual, including the types of information specifically described in section 3 of the *Privacy Act*, R.S. 1985, c. P-21;

"Record" means any hard copy document or any data in a machine-readable format containing Personal Information;

ii. Words and expressions defined in the General Conditions and used in this Article have the meanings given to them in the General Conditions.

iii. If there is any inconsistency between the General Conditions and these privacy articles, the applicable provision of these privacy articles will prevail.

b. Ownership of Personal Information and Records

To perform the Work, the Contractor will be provided with and/or will be collecting Personal Information from third parties. The Contractor acknowledges that it has no rights in the Personal Information or the Records. On request, the Contractor must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

c. Use of Personal Information

The Contractor agrees to create, collect, receive, manage, access, use, retain, disclose and dispose of the Personal Information and the records only to perform the Work in accordance with the Contract and must do so in accordance with this Contract.

d. Collection of Personal Information

The Contractor is only authorized to collect Personal Information listed in the Security Requirements Checklist (SRCL), Annex 4. In the event the Contractor is required to collect additional Personal Information to perform the Work under the Contract, the Contractor must seek and receive written approval from the Project Authority before collecting additional elements of Personal Information.

If the Contractor must collect Personal Information from a third party to perform the Work, the Contractor must only collect Personal Information that is required to perform the Work. The Contractor must collect the Personal Information from the individual to

whom it relates and the Contractor must inform that individual (at or before the time when it collects the Personal Information) of the following:

i. that the Personal Information is being collected on behalf of, and will be provided to, Canada;
ii. the ways the Personal Information will be used;
iii. that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;
iv. the consequences, if any, of refusing to provide the information;
v. that the individual has a right to access and correct his or her own Personal Information; and
vi. that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act)*, and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the Contractor.

The Contractor, its subcontractors, and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

If requested by the Contracting Authority, the Contractor must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The Contractor must not begin using a form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

At the time it requests Personal Information from any individual, if the Contractor doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the Contractor must ask the Contracting Authority for instructions.

e. Maintaining the Accuracy, Privacy and Integrity of Personal Information

The Contractor must ensure that the Personal Information is as accurate, complete, and up to date as possible. The Contractor must protect the privacy of the Personal Information. To do so at a minimum, the Contractor must:

i. not use any personal identifiers (e.g., social insurance number, passport number, unique client identifiers) to link multiple databases containing Personal Information;

ii. segregate all Records from the Contractor's own information and Records;

iii. restrict access to the Personal Information and the Records to people who require access to perform the Work (for example, by using passwords or biometric access controls);

iv. provide training to anyone to whom the Contractor will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Work. The Contractor must provide this training before giving an individual access to any Personal Information and the Contractor must keep a record of the training and make it available to the Contracting Authority if requested;

v. if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the Contractor provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

vi. keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

vii. include a notation on any Record(s) that an individual has requested be corrected if the Contractor has decided not to make the correction for any reason. Whenever this occurs, the Contractor must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the Contractor's decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

viii. keep a record of the date and source of the last update to each Record;

ix. maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the Contractor and Canada at any time; and

x. secure and control access to any Personal Information.

f. Safeguarding Personal Information

The Contractor must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. In doing so, the Contractor must implement administrative, physical and technical security and safeguarding measures and solutions to preserve the confidentiality, security and integrity of premises, Personal Information and systems. These measures and solutions must satisfy all requirements described in the Contract, including Annex 2 – Security and Privacy and Annex 1 – Statement of Work, including compliance with principles of privacy laws referred to herein and any relevant Government of Canada

directives, standards, guidelines, protocols and policies. These measures and solutions must also comply with industry standards or best practices whichever offers greater protection. Canada reserves the right to request implementation of additional reasonable measures and solutions from time to time. To do so, at a minimum, the Contractor must:

i. store the Personal Information electronically so that a password (or a similar access control mechanism) is required to access the system or database in which the Personal Information is stored

ii. ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;

iii. not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Contracting Authority has first consented in writing;

iv. safeguard any database or computer system on which the Personal Information is stored from external access in order to protect highly secure or sensitive information;

v. maintain a secure back-up copy of all Records, updated at least weekly;

vi. implement any reasonable security or protection measures requested by Canada from time to time; and

vii. notify the Contracting Authority immediately of any suspected or confirmed security breaches; for example, including but not limited to: unauthorized access, use, disclosure of Personal Information; or an incident that may jeopardize the security or integrity of Records; or the systems or facilities where Personal Information is held. In the event of any security breach, the Contractor and/or any and all subcontractors shall immediately take all reasonable steps to limit or contain scope of the breach, resolve the problem and prevent its recurrence. Canada may direct the Contractor to take specified steps to resolve and prevent a recurrence, and in addition may rely upon the provisions of this Contract relating to suspension or termination for default.

g. Appointment of Privacy Officer

The Contractor must appoint someone to be its privacy officer and to act as its representative for all matters related to the Personal Information and the Records. The Contractor must provide that person's name to the Contracting Authority within ten (10) working days of the award of the Contract.

h. Quarterly Reporting Obligations

Within thirty (30) calendar days of the end of each quarter (January-March; April-June; July-September; October-December), the Contractor must submit the following to the Contracting Authority:

i. a description of any new measures taken by the Contractor to protect the Personal Information (for example, new software or access controls being used by the Contractor);

ii. a list of any corrections made to Personal Information at the request of an individual (including the name of the individual, the date of the request, and the correction made);

iii. details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; and

iv. a complete copy (in an electronic format agreed to by the Contracting Authority and the Contractor) of all the Personal Information stored electronically by the Contractor.

i. Audit

Canada may audit the Contractor's compliance with these privacy articles at any time. If requested by the Contracting Authority, the Contractor must provide Canada (or Canada's authorized representative) with access to its premises or that of a subcontractor and to the Personal Information and Records at all reasonable times. If Canada identifies any deficiencies during an audit, the Contractor must immediately correct the deficiencies at its own expense.

j. Statutory Obligations

i. The Contractor acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's ***Privacy Act***, ***Access to Information Act***, R.S. 1985, c. A-1, and ***Library and Archives of Canada Act***, S.C. 2004, c. 11. The Contractor agrees to comply with any requirement established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

ii. The Contractor acknowledges that its obligations under the Contract are in addition to any obligations it has under the ***Personal Information Protection and Electronic Documents Act***, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the Contractor believes that any obligations in the Contract prevent it from meeting its obligations under any of these laws, the Contractor must immediately notify the Contracting Authority of the specific provision of the Contract and the specific obligation under the law with which the Contractor believes it conflicts.

k. Disposing of Records and Returning Records to Canada

The Contractor must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Work involving the Personal Information is complete, the Contract is complete, or the Contract is terminated, whichever of these comes first, the Contractor must return any remaining Records (including all copies) to the Contracting Authority.

l. Legal Requirement to Disclose Personal Information

Before disclosing any of the Personal Information pursuant to any applicable legislation, regulation, or an order of any court, tribunal or administrative body with jurisdiction, the Contractor must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

m. Complaints

Canada and the Contractor each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

n. Exception

The obligations set out in these privacy articles do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.

7.6 On-going Supply Chain Integrity Process

7.6.1 **Supply Chain Integrity Process**: The Parties acknowledge that a Supply Chain Integrity Process assessment was a key component of the procurement process that resulted in the award of this Contract. In connection with that assessment process, Canada assessed the Contractor's Supply Chain Security Information (SCSI) without identifying any security concerns. The following SCSI was submitted:

i. an IT Product List;
ii. a list of subcontractors; and
iii. network diagram(s).

This SCSI is included as Annex (to be confirmed at contract award). The Parties also acknowledge that security is a critical consideration for Canada with respect to this contract and that on-going assessment of SCSI will be required throughout the contract Period. This Article governs that process.

7.6.2 **Assessment of New SCSI**: During the Term of Contract, the Contractor may need to modify the SCSI information contained in Annex (to be confirmed at contract award). In that regard:

a. The Contractor, starting at contract award, must revise its SCSI at least once a month to show all changes made, as well as all deletions and additions to the SCSI that affect the services under the Contract (including Products deployed by its subcontractors) during that period; the list must be marked to show the changes made during the applicable period. If no changes have been made during the reporting month, the Contractor must advise the Contracting Authority in writing that the existing list is unchanged. Changes

made to the IT Product List must be accompanied with revised Network Diagram(s) when applicable.

b. The Contractor agrees that, during the Term of Contract, it will periodically (at least once a year) provide the Contracting Authority with updates regarding upcoming new Products that it anticipates deploying in the Work (for example, as it develops its "technology roadmap" or similar plans). This will allow Canada to assess those Products in advance so that any security concerns can be identified prior to the Products being deployed in connection with the services being delivered under the Contract. Canada will endeavour to assess proposed new Products within 30 calendar days, although lengthier lists of Products may take additional time.

c. Canada reserves the right to conduct a complete, independent security assessment of all new SCSI. The Contractor must, if requested by the Contracting Authority, provide any information that Canada requires to perform its assessment.

d. Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is provided by the Contractor or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of any proposed new SCSI.

7.6.3 Identification of New Security Vulnerabilities in SCSI already assessed by Canada:

a. The Contractor must provide to Canada timely information about any vulnerabilities of which it becomes aware in performing the Work, including any weakness, or design deficiency, identified in any Product used to deliver services that would allow an unauthorized individual to compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications it hosts.

b. The Contractor acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified and, that being the case, new security vulnerabilities may be identified in SCSI that have already been the subject of an SCSI assessment and assessed without security concerns by Canada, either during the procurement process or later during the contract Period.

7.6.4 Addressing Security Concerns:

a. If Canada notifies the Contractor of security concerns regarding a Product that has not yet been deployed, the Contractor agrees not to deploy it in connection with this contract without the consent of the Contracting Authority.

b. At any time during the Term of Contract, if Canada notifies the Contractor that, in Canada's opinion, there is a Product that is being used in the Contractor's solution (including use by a subcontractor) that has been assessed as having the potential to compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, then the Contractor must:

i. provide Canada with any further information requested by the Contracting Authority so that Canada may perform a complete assessment;

ii. if requested by the Contracting Authority, propose a mitigation plan (including a schedule), within 10 business days, such as migration to an alternative Product. The Contracting Authority will notify the Contractor in writing if Canada approves the mitigation plan, or will otherwise provide comments about concerns or deficiencies with the mitigation plan; and

iii. implement the mitigation plan approved by Canada.

c. This process applies both to new Products and to Products that were already assessed pursuant to the Supply Chain Integrity Process assessment by Canada, but for which new security vulnerabilities have since been identified.

d. Despite the previous sub-article, if Canada determines in its discretion that the identified security concern represents a threat to national security that is both serious and imminent, the Contracting Authority may require that the Contractor immediately cease deploying the identified Product(s) in the Work. For Products that have already been deployed, the Contractor must identify and/or remove (as required by the Contracting Authority) the Product(s) from the Work according to a schedule determined by Canada. However, prior to making a final determination in this regard, Canada will provide the Contractor with the opportunity to make representations within 48 hours of receiving notice from the Contracting Authority. The Contractor may propose, for example, mitigation measures for Canada's consideration. Canada will then make a final determination.

7.6.5 General:

a. The process described in this Article may apply to a single Product, to a set of Products, or to all Products manufactured or distributed by a particular supplier.

b. The process described in this Article also applies to subcontractors. With respect to cost implications, Canada acknowledges that the cost considerations with respect to concerns about subcontractors (as opposed to Products) may be different and may include factors such as the availability of other subcontractors to complete the work.

c. Any service levels that are not met due to a transition to a new Product or subcontractor required by Canada pursuant to this Article will not trigger a Service Credit, nor will a failure in this regard be taken into consideration for overall metric calculations, provided that the Contractor implements the necessary changes in accordance with the migration plan approved by Canada or proceeds immediately to implement Canada's requirements if Canada has determined that the threat to national security is both serious and imminent.

d. If the Contractor becomes aware that any subcontractor is deploying Products subject to security concerns in relation to the Work, the Contractor must immediately notify both the Contracting Authority and the Technical Authority and the Contractor must enforce the terms of its contract with its subcontractor. The Contractor acknowledges its obligations pursuant to General Conditions 2035, Subsection 8(3).

e. Any determination made by Canada will constitute a decision with respect to a specific Product or subcontractor and its proposed use under this Contract, and does not mean that the same Product or subcontractor would necessarily be assessed in the same way if proposed to be used for another purpose or in another context.

7.6.6 Subcontracting

a. Despite the General Conditions, none of the Work may be subcontracted (even to an affiliate of the Contractor) unless the Contracting Authority has first consented in writing. In order to seek the Contracting Authority's consent, the Contractor must provide the following information:

   i. the name of the subcontractor;

   ii. the portion of the Work to be performed by the subcontractor;

   iii. the Designated Organization Screening or the Facility Security Clearance (FSC) level of the subcontractor;

   iv. the date of birth, the full name and the security clearance status of individuals employed by the subcontractor who will require access to Canada's facilities;

   v. completed sub-SRCL signed by the Contractor's Company Security Officer for CISD completion; and

   vi. any other information required by the Contracting Authority.

b. For the purposes of this Article, a "subcontractor" does not include a supplier who deals with the Contractor at arm's length whose only role is to provide telecommunications or

other equipment or software that will be used by the Contractor to provide services, including if the equipment will be installed in the backbone or infrastructure of the Contractor.

7.6.7 Change of Control

a. At any time during the Term of Contract, if requested by the Contracting Authority, the Contractor must provide to Canada:

i. an organization chart for the Contractor showing all related corporations and partnerships; for the purposes of this sub-article, a corporation or partnership will be considered related to another entity if:

1. they are "related persons" or "affiliated persons" according to the Canada *Income Tax Act;*
2. the entities have now or in the two years before the request for the infor*mation had a fid*uciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or
3. the entities otherwise do not deal with one another at arm's length, or ea*ch of them does* not deal at arm's length with the same third party.

ii. a list of all the Contractor's shareholders; if the Contractor is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; with respect to any publicly traded corporation, Canada anticipates that the circumstances in which it would require a complete list of shareholders would be unusual and that any request from Canada for a list of a publicly traded corporation's shareholders would normally be limited to a list of those shareholders who hold at least 1% of the voting shares;

iii. a list of all the Contractor's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the Contractor is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; and

iv. any other information related to ownership and control that may be requested by Canada.

b. If requested by the Contracting Authority, the Contractor must provide this information regarding its subcontractors as well. However, if a subcontractor considers this information to be confidential, the Contractor may meet its obligation by having the subcontractor submit the information directly to the Contracting Authority. Regardless of whether the information is submitted by the Contractor or a subcontractor, Canada agrees to handle this information in accordance with Subsection 22(3) of General Conditions 2035 (General Conditions – Higher Complexity – Services), provided the information has been marked as either confidential or proprietary.

c. The Contractor must notify the Contracting Authority in writing of:

i. any change of control in the Contractor itself;

ii. any change of control in any parent corporation or parent partnership of the Contractor, up to the ultimate owner; and

iii. any change of control in any subcontractor performing any part of the Work (including any change of control in any parent corporation or parent partnership of the subcontractor, up to the ultimate owner).

d. The Contractor must provide this notice by no later than 10 working days after any change of control takes place (or, in the case of a subcontractor, within 15 working days after any change of control takes place). Where possible, Canada requests that the Contractor provide advance notice of any proposed change of control transaction.

e. In this Article, a "change of control" includes but is not limited to a direct or indirect change in the effective control of the corporation or partnership, whether resulting from a sale, encumbrance, or other disposition of the shares (or any form of partnership units) by any other means. In the case of a joint venture Contractor or subcontractor, this applies to a change of control of any of the joint venture's corporate or partnership members. In the case of a Contractor or subcontractor that is a partnership or limited partnership, this requirement also applies to any corporation or limited partnership that is a partner.

f. If Canada determines in its sole discretion that a change of control affecting the Contractor (either in the Contractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada may terminate the contract on a "no-fault" basis by providing notice to the Contractor within 90 days of receiving the notice from the Contractor regarding the change of control. Canada will not be required to provide its reasons for terminating the contract in relation to the change of control, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security.

g. If Canada determines in its sole discretion that a change of control affecting a subcontractor (either in the subcontractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada will notify the Contractor in writing of its determination. Canada will not be required to provide the reasons for its determination, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security. The Contractor must, within 90 days of receiving Canada's determination, arrange for another subcontractor, acceptable to Canada, to perform the portion of the Work being performed by the existing subcontractor (or the Contractor must perform this portion of the Work itself). If the Contractor fails to do so within this time period, Canada will be entitled to terminate the contract on a "no-fault" basis by providing notice to the Contractor within 180 days of receiving the original notice from the Contractor regarding the change of control.

h. In this Article, termination on a "no-fault" basis means that neither party will be liable to the other in connection with the change of control or the resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

i. Despite the foregoing, Canada's right to terminate on a "no-fault" basis will not apply to circumstances in which there is an internal reorganization that does not affect the

ownership of the ultimate parent corporation or parent partnership of the Contractor or subcontractor, as the case may be; that is, Canada does not have a right to terminate the contract pursuant to this Article where the Contractor or subcontractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner. However, in any such case, the notice requirements of this Article still apply.

7.7 Term of Contract

7.7.1 **Period of the Contract**: The Contract begins on the date of contract award and ends 7 years later.

7.7.2 **Option to Extend the Contract**

a. The Contractor grants to Canada the irrevocable Option(s) to extend the Period of the Contract by up to 5 years, in increments of 1 year, under the same conditions. The Contractor agrees that, during the extended Period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

b. Canada may exercise this option at any time. To exercise an Option, Canada will send a written notice to the Contractor at least 6 months before the expiry date of the Contract. The Option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.8 Authorities

7.8.1 Contracting Authority

The Contracting Authority for the contract is: (to be confirmed at contract award)

Name: _____
Title: _____
Public Works and Government Services Canada
Acquisitions Branch
Directorate: _____
Address: _____

Telephone:___-___-_____
Facsimile:___-___-_____
E-mail address:_____

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.8.2 Project Authority

The Project Authority for the contract is: (to be conformed at contract award)

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone:___-___-_____
Facsimile:___-___-_____
E-mail address:_____

The Project Authority, or an authorized delegate, is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

7.8.3 Contractor's Representative and Executive Authority(to be confirmed at contract award)

The Contractor's Representative and Executive Authority for the contract is:

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone:___-___-_____
Facsimile:___-___-_____
E-mail address:_____

The Contractor must identify a representative who will act as the Executive Authority (EA) and will hold the highest level of resolution and approval authority on behalf of the Contractor. The EA should be available during core business hours EST at the request of the Contracting and Project Authority.

7.9 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a *Public Service Superannuation Act* (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.10 Term of Payment

7.10.1 Basis of Payment

(i) e-Procurement Solution Transition-In Fee

a. EPS Transition-In Fee:

For the entirety of the Work described in Part 6, section 6.3 to 6.5 of the Statement of Work in Annex 1:

As consideration to the Contractor for satisfactorily completing its obligations under the Contract, Canada will pay the Contractor an EPS Transition-In Fee of $_____ which is a firm lump sum fee, customs duties included and Applicable Taxes extra. The EPS Transition-In Fee is divided into milestones as set out in the Schedule of Milestones detailed in Annex 3 – Price Schedule. Each EPS Transition-In Fee milestone amount is payable only after completion of the respective milestone to which the milestone amount applies.

(ii) e-Procurement Solution Operational Fee:

The EPS Operational Fee is consideration for all authorized Work in accordance with all sections of the Statement of Work with the exception of Part 6, section 6.3 to 6.5 and Part 7 of the Statement of Work in Annex 1.

The EPS Operational Fee, as described below, is payable monthly from the Operational Start Date to the Operational End Date. The applicable EPS Operational Fee in any given month will be determined by the highest number of Users of the EPS in that month, as follows:

a. EPS Operational Fee – Tier 1: 1 to 5,000 Users – Monthly Lump Sum Fee

EPS Operational Fee – Tier 1 is a lump sum monthly fee applicable where there is 1 to 5,000 Users of the EPS in that month.

(A) EPS Operational Fee – Tier 1: Monthly Lump Sum Fee of $_____, Customs duties are included and Applicable Taxes are extra.

b. EPS Operational Fee – Tier 2: in excess of 5,000 Users – Firm Monthly Rate per User

EPS Operational Fee – Tier 2 is a firm monthly rate per User for Users of the EPS in a given month in excess of 5,000 Users.

(B) EPS Operational Fee – Tier 2: Firm Monthly Rate per User of $_____, Customs duties are included and Applicable Taxes are extra.

c. EPS Operational Fee – Tier 3: Unlimited Users – Monthly Lump Sum Fee

EPS Operational Fee – Tier 3 is a lump sum monthly fee for unlimited number of Users of the EPS system in that month.

(C) EPS Operational Fee – Tier 3: Monthly Lump Sum Fee of $_____, Customs duties are included and Applicable Taxes are extra.

Canada reserves the right to apply either the EPS Operational Fee Tier 1 and Tier 2 or, in lieu, apply EPS Operational Tier 3. Where Canada opts to change from either Tier 1 and Tier 2 to Tier 3, or vice versa, as the basis of payment utilised for EPS Operational Fee in effect under the Contract, it will give the Contractor a minimum two months advance notice.

It is agreed and understood by both Parties that it is a condition of the Contract that Canada has the right to:

(A) De-list User(s) who use and have access to the EPS and/or receive Maintenance and Support, Training and Help Desk services for the EPS, at any time during the Term of the Contract, solely at Canada's discretion and at no cost.

(B) Subject to de-listing User(s) as stated in (A) above, Canada has the right to transfer and reallocate the paid portion of unused User fees to new User(s) at any time within the same quarter, solely at Canada's discretion and at no cost;

(C) The Contractor agrees to provide all services covered by the User fees at no additional cost, if the transfer and reallocation of already paid User fees is to a new User(s) not already covered by a User fee;

(D) Canada has the right, at any time during the Term of the Contract, to readjust (increase or decrease) the total number of Users that are entitled to receive all services covered by the User fees.

(iii) Optional Services Fees

a. Optional Work – Fixed Prices:

For the Work described in section *7.2.3 – Tender Feeds* and *7.2.4 – Data Escrow* of the Statement of Work in Annex 1:

As consideration to the Contractor satisfactorily completing all of its obligations under the authorized Task Authorization (TA), Canada will pay the Contractor the following Fixed Prices *in accordance with Annex X – Basis of Payment*, as specified in the authorized TA:

(A) Tender Feeds $_____; and
(B) Data Escrow $_____.

Customs duties are included and Applicable Taxes are extra.

The Work covered by the Optional Work – Fixed Prices can be requested at any time by Canada during the entire Term of the Contract.

b. Professional Services provided under a Task Authorization – Firm Per Diem Rates:

Using a Task Authorization (TA), for the Work described in section *7.1 – Optional Professional Services As and When Required* of the Statement of Work in Annex 1, and only where the Work is not otherwise covered by another section of the SOW:

Professional Services provided under a Task Authorization: Firm Per Diem Rate: For professional services, as and when requested by Canada during the Term of the Contract, including any extensions to it exercised as options by the Contracting Authority in accordance with the Contract, and in accordance with an authorized Task Authorization, Canada will pay the Contractor in arrears and no more than once a month, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables in accordance with the firm all-inclusive per diem rates in accordance with the prices included in Annex X – Basis of Payment. Customs duties are included and Applicable Taxes are extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.

Estimated Cost $_____.

Work of the TA: The Work described in the TA must be in accordance with the scope of the Contract and can be requested at any time by Canada during the entire Term of the Contract.

Pre-Authorized Travel and Living Expenses: Canada will not reimburse the Contractor for travel and living expenses incurred to perform the Work in the National Capital Region, nor will Canada reimburse for travel and living expenses incurred to travel from the Contractor's location to and from the National Capital Region. These costs must be part of the firm per diem rate. The Contractor will be able to charge for time spent travelling from the National Capital Region to Canada's work site(s), at the per diem rates set out in the Contract, for Work outside the National Capital Region. Canada will reimburse the Contractor for its pre-authorized travel and living expenses reasonably and properly incurred in the performance of the Work outside the National Capital Region, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B, C and D of the Treasury Board Travel Directive, and with the other provisions of the directive referring to "travellers", rather than those referring to "employees". All travel must have the prior authorization of the Technical Authority. All payments are subject to government audit.

Competitive Award: The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

Professional Services Rates: In Canada's experience, bidders from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. This denies Canada of the benefit of the awarded contract. If the

Contractor refuses, or is unable, to provide an individual with the qualifications described in the Contract within the time described in the Contract (or proposes instead to provide someone from an alternate category at a different rate), whether or not Canada terminates the Contract as a whole, Canada may impose sanctions or take other measures in accordance with the PWGSC Vendor Performance Policy (or equivalent) then in effect, which may include prohibiting the Contractor from bidding on future requirements that include any professional services, or rejecting the Contractor's other bids for professional services requirements on the basis that the Contractor's performance on this or other contracts is sufficiently poor to jeopardize the successful completion of other requirements.

Purpose of Estimates: All estimated costs contained in the Contract are included solely for the administrative purposes of Canada and do not represent a commitment on the part of Canada to purchase goods or services in these amounts. Any commitment to purchase specific amounts or values of services are described elsewhere in the Contract.

c. Option for Third Party Integration:

For the Work described in section *7.2.2 – Third Party Integration* of the Statement of Work in Annex 1:

In consideration of the Contractor satisfactorily completing all of its obligations under the authorized Task Authorization (TA), Canada will pay the Contractor the agreed upon negotiated price, as specified in the authorized TA.

d. Option for Other Public Sector Entities:

For the Work described in section *7.3.2 – Option for Other Canadian Public Sector Entities to acquire an EPS* of the Statement of Work in Annex 1:

In consideration of the Contractor satisfactorily completing all of its obligations under the authorized Task Authorization (TA), Canada will pay the Contractor the agreed upon negotiated price, as specified in the authorized TA.

7.10.2 Limitation of Expenditure

(i) Canada's total liability to the Contractor under the Contract must not exceed the amount set out on page 1 of the Contract. The amount set out on page one of the Contract has been calculated as the sum of the following:

(A) $_____, for the e-Procurement Solution Transition-In Fee;

(B) $_____, for the e-Procurement Solution Operational Fee, comprised of the following:

i. $_____, for 1 to 5,000 Users

AND

$_____, for Users in excess of 5,000
(#___Users in excess of 5,000 x $_(firm monthly rate per User)

OR

ii. $_____, for unlimited Users; and

(C) $_____, for Optional Services Fees, comprised of the following:

i. $_____, for Optional Work Prices

AND

$_____, for Professional Services as-and-when requested though the Task Authorization process.

Applicable Taxes are extra, as applicable.

Note to Bidders: *The above information will be completed prior to Contract award.*

These amounts has been included for the administrative purposes of Canada and does not represent a commitment to purchase services under this Contract in these amounts. Canada retains the right to manage these amounts, as required and in accordance with the Contract, as long as the total Limitation of Expenditure for the Contract, or for the individual Option Period(s), is not exceeded for the period in which the respective estimates apply.

(ii) No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

(1) When it is 75 percent committed, or
(2) 4 months before the Contract expiry date, or
(3) as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Providing this information does not increase Canada's liability.

7.10.3 Method of Payment – e-Procurement Solution Transition-In Fee

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract if:

a. an accurate and complete claim for payment using form PWGSC-TPSGC 1111, Claim for Progress Payment, and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
c. all the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives;
d. all work associated with the milestone and as applicable any deliverable required have been completed and accepted by Canada.

7.10.4 Method of Payment – e-Procurement Solution Operational Fee

Tier 1, Tier 2 and Tier 3 EPS Operation Fee

Canada will pay the Contractor, in arrears on a monthly basis, for the Work covered by the EPS Operational Fee, if:

a. an accurate and complete invoice, the user count report (as described in Part 6, section 6.3.5.4 of the Statement of Work in Annex 1) and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b. all such documents have been verified by Canada; and
c. the Work has been delivered and accepted by Canada.

7.10.5 Method of Payment – Optional Services Fees

For any TA issued under this Contract, Canada will pay the Contractor in accordance with one of the following methods. Canada retains the right to select any of the following methods but may consult the Contractor at time of issuance of the TA:

(i) Method of Payment for Task Authorization with Firm Price - Lump Sum Payment on Completion: For any authorized Task Authorization issued under the Contract that contains a Lump Sum Payment on Completion, Canada will pay the Contractor upon completion and delivery of all the Work associated with the Task Authorization in accordance with the payment provisions of the Contract if:

a. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b. all such documents have been verified by Canada; and,

c. the Work delivered has been accepted by Canada.

(ii) Method of Payment for Task Authorization with Firm Prices - Milestone Payment: For any authorized Task Authorization issued under the Contract that includes a schedule of milestone payments to be made once specific portions of the work have been completed and accepted, Canada will make milestone payments in accordance with the schedule of milestones detailed in that TA and the payment provisions of the Contract:

a. an accurate and complete claim for milestone payment using form PWGSC-TPSGC 1111http://www.pwgsc.gc.ca/acquisitions/text/forms/forms-e.htmlCa/acquisitions/text/forms/forms-e.html) and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b. all the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives; and
c. all work associated with the milestone and any deliverable required have been completed, delivered, and accepted by Canada.

(iii) Method of Payment for Task Authorizations with a Maximum Price: For any authorized Task Authorization issued under the Contract that contains a maximum price:

a. Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment. The Contractor must submit time sheets for each resource showing the days and hours worked to support the charges claimed in the invoice; and

b. Once Canada has paid the maximum TA price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the issued TA, all of which is required to be performed for the maximum TA price. If the work described in the TA is completed in less time than anticipated, and the actual time worked (as supported by the time sheets) at the rates set out in the Contract is less than the maximum price, Canada is only required to pay for the time spent performing the work related to that TA.

7.10.6 No Responsibility to Pay for Work not Performed due to Closure of Government Offices

(i) Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.

(ii) If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises.

7.10.7 No Additional Fees for Third Party Use of the EPS

(i) No fees can be charged to third parties (Canadians and non-Canadians, employees and Contractors of Canada – regardless of their location and/or jurisdiction) for any functionalities and services made available by the Work described in the SOW, including for accessing and using the EPS through Internet, intranet and extranet environments or any other connections to use the services and programs provided by the EPS, including: accessing, viewing, entering, searching, exchanging and reading information held and created by the Client.

7.10.8 Performance Incentive Fee

(i) The objective of the Performance Incentive Fee (PIF) is to encourage the Contractor to pro-actively assist Canada in achieving outstanding results in areas the Government has chosen for special emphasis or priority.

(ii) The PIF is a discretionary program, at Canada's sole discretion. Prior to the beginning of each Fiscal Year, Canada will determine whether a PIF will be put in place for that year to support the achievement of any special objectives or priorities it may have. The Project Authority (PA) will consult with the Contractor and then notify the Contractor of any PIF that is to be made available using a Letter of Emphasis.

(iii) As a prerequisite to being considered eligible for a PIF discretionary payment, the Contractor must first have met the minimum Service Levels for the Fiscal Year.

(iv) The total PIF payments in a given Fiscal Year can be no greater than 10% of the total possible Contract fees for that Fiscal Year. The total of all PIF payments over the life of the contract can be no greater than 10% of the total of all Fees paid in all fiscal years.

(v) The Letter of Emphasis will identify target PIF initiatives and set out specific objectives that are to be emphasized, the performance measurement criteria that will be used to assess the achievement of those objectives, the percentage of Contract Fees available as the PIF payment and the allocation of that percentage between objectives. The PA will seek input from the Contractor regarding the selection of areas of emphasis, but the final selection of these will be at the sole discretion of the PA.

(vi) PIF-related performance will be assessed against the areas set out in the Letter of Emphasis. The Contractor will prepare a monthly status report to provide feedback on progress towards meeting the objectives and the performance measurement criteria. At the end of the Fiscal Year, the PA will use the final year-end status report to determine whether the Contractor has met the objectives and is eligible for the PIF payment

(vii) In the event the Contractor has passed all the KPIs for the Fiscal Year and the PIF objectives and performance measurement criteria have been met, the PA will authorize the PIF payment. The PIF payment will be calculated by multiplying the total Contract Fees for that Fiscal Year by the percentage of Contract Fees available for the PIF payment identified in the Letter of Emphasis.

(viii) In the event the Contractor has met all the Service Levels for the Fiscal Year but only some of the PIF objectives and performance measurement criteria have been met, the PA will authorize a partial PIF payment based on the allocations for those objectives set out in the Letter of Emphasis.

(ix) All PIF amounts are payable at Canada's sole discretion and are not subject to any dispute resolution sections of the Contract.

(x) Canada is not bound to use any PIF nor is it bound to use the entire amount of any PIF that is put in place.

7.10.9 Service Level Failure Penalties and Earn-Backs

(i) Payment Credits

Credits for Failure to Meet Minimum Service Level: If the Contractor does not meet the minimum Service Levels at any given time during the Term of the Contract, the Contractor agrees to pay Canada a credit. The total amount of Payment Credits shall not exceed 10% of the payment made by Canada for the month within which the Payment Credits occurred. The minimum Service Levels and the Payment Credits are specified in Part 3, section 3.7.4 and 3.7.8 and Part 6, section 6.10 in Annex 1 – Statement of Work.

Corrective Measures: If Payment Credits are payable under this Article for two consecutive months or for three months in any 12-month period, Canada reserves the right to escalate payment credits to 30% of the payment made by Canada for the month within which the Payment Credits occurred. Furthermore, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake to eliminate the recurrence of the problem. The Contractor will have the first five working days of the following month to deliver the action plan to the Project Authority and the Contracting Authority and the remainder of the calendar month to rectify the underlying problem and meet the required Service Levels.

(ii) Credits Apply during Entire Term of the Contract: The Parties agree that the credits apply throughout the Term of the Contract.

(iii) Credits represent Liquidated Damages: The Parties agree that the credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

(iv) Canada's Right to Obtain Payment: The Parties agree that these credits are a liquidated debt. To collect the credits, Canada has the right to hold back, draw back, deduct or set off from and against any money Canada owes to the Contractor from time to time.

(v) Canada's Rights & Remedies not Limited: The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

(vi) Audit Rights: The Contractor's calculation of credits under the Contract is subject to verification by government audit, at the Contracting Authority's discretion, before or after payment is made to the Contractor. The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately credited to Canada in the Contractor's invoices. If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year). If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

(vii) Earn-Back

Following any service level failure, Canada may allow the Contractor the opportunity to earn back the Payment Credits charged in one or more measurement period. If all the service levels for the relevant service and any others agreed to be associated with that service are met, or exceeded, during each of the three measurement periods following the service level failure, Canada may, at its sole discretion, return half of the Payment Credits paid to the Contractor. If all the service levels for the relevant service and any others agreed to be associated with that service are met, or exceeded, during each of the six measurement periods following the service level failure, Canada may, at its sole discretion, return the remaining half of the Payment Credits paid to the Contractor. The Contractor may, where the requisite levels of performance are achieved, make representations to Canada in this regard.

(viii) Review of Service Levels

On an as-needed basis after the initial baseline service levels have been established, Canada can request a change to any service level by providing notice to the Contractor that a service level needs to be changed. This change can take effect only after the Contractor has had sufficient time to review the requested change and determine if any modifications are required to the delivery of services. Should changes be required by the Contractor, then Canada must allow the Contractor reasonable time to make such changes before the service level change takes place.

(ix) Baseline Service Level Timing

On a quarterly basis beginning six months after the date of Contract award, Canada and the Contractor must review the service levels, and agree to adjustments to them or new requirements as appropriate.

7.11 Annual Inflation Adjustment

The e-Procurement Solution Operational Fee and all Professional Services Per Diem Rates are subject to an annual inflation adjustment as of April 1, 2020. The adjustment will be equal to the increase in the all-items Consumer Price Index, monthly (CANSIM Table 326-0020) for January of that year over the same Index for the previous January**,** as published by Statistics Canada for the previous year. Any subsequent adjustments will be calculated on the most recent previous e-Procurement Solution Operational Fee and Professional Services Per Diem Rate. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

7.12 Exchange Rate Fluctuation Adjustment

7.12.1 The foreign currency component (FCC) is defined as the portion of the price or rate that will be directly affected by exchange rate fluctuation. The FCC should include all related taxes, duties and other costs paid by the Bidder and which are to be included in the adjustment amount.

7.12.2 For each line item where a FCC is identified, Canada assumes the risks and benefits for exchange rate fluctuation, as shown in the Basis of Payment. For such items, the exchange rate fluctuation amount is determined in accordance with the provision of this clause.

7.12.3 The total price paid by Canada on each invoice will be adjusted at the time of payment, based on the FCC and the exchange rate fluctuation provisions in the contract. The exchange rate adjustment amount will be calculated in accordance with the following formula:

Adjustment = FCC x Qty x $(i_1 - i_0) / i_0$
where formula variables correspond to:

FCC: Foreign Currency Component (per unit)
$\mathbf{i_0}$: initial exchange rate (CAN$ per unit of foreign currency [e.g. US$1])
$\mathbf{i_1}$: exchange rate for adjustments (CAN$ per unit of foreign currency [e.g. US$1])
Qty: quantity of units

7.12.4 The initial exchange rate is typically set as the noon rate as published by the Bank of Canada on the solicitation closing date.

7.12.5 For goods, the exchange rate for adjustment will be the noon rate as published by the Bank of Canada on the date the goods were delivered. For services, the exchange rate for adjustment will be the noon rate on the last business day of the month for which the services were performed. For advance payments, the exchange rate for adjustment will be the noon rate on the date the payment was due. The most recent noon rate will be used for non-business days.

7.12.6 The Contractor must indicate the total exchange rate adjustment amount (either upward, downward or no change) as a separate item on each invoice or claim for payment submitted under the Contract. Where an adjustment applies, the Contractor must submit with their invoice form PWGSC-TPSGC 450, Claim for Exchange Rate Adjustments.

7.12.7 The exchange rate adjustment will only be applied where the exchange rate fluctuation is greater than 2% (increase or decrease), calculated in accordance with column 8 of form PWGSC-TPSGC 450 (i.e. $[i_1 - i_0) / i_0]$).

7.12.8 Canada reserves the right to audit any revision to costs and prices under this clause.

7.13 Invoicing Instructions

a. The Contractor must submit invoices in accordance with the information required in the 2035 General Conditions.

b. The Contractor's invoice must include a separate line item for each subparagraph in the provisions of Annex 3 - Price Schedule.

c. By submitting invoices, the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Price Schedule provisions in Annex 3 of the Contract, including any charges for work performed by subcontractors.

d. The Contractor must provide the original of each invoice to the Project Authority. On request, the Contractor must provide a copy of any invoices requested by the Contracting Authority.

e. The Contractor must submit a detailed monthly cumulative expenditure tracking report to the Project Authority for approval.

f. The Contractor must submit a copy of the detailed monthly cumulative expenditure tracking report to the Contract Authority, as approved by the Project Authority.

7.14 Certifications

The continuous compliance with the certifications provided by the Contractor in its bid and the ongoing cooperation in providing associated information are conditions of the Contract. Certifications are subject to verification by Canada during the entire period of the Contract. If the Contractor does not comply with any certification, fails to provide the associated information, or if it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

7.15 Federal Contractors Program for Employment Equity - Default by the Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.16 Applicable Laws

The contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

7.17 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

a. the Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement

b. the supplemental general conditions,

i. 4006 (2010-08-16), Supplemental General Conditions- Contractor to Own Intellectual Property Rights in Foreground Information; and
ii. 4008 (2008-12-12), Supplemental General Conditions- Personal Information.

c. the general conditions

i. 2035 (2015-07-03), General Conditions - Higher Complexity - Services
ii. Annex 1 – Statement of Work;
iii. Annex 2 – Security and Privacy;
iv. Annex 3 – Price Schedule;
v. Annex 4 – Security Requirements Check List and Security Classification Guide
vi. Annex 5 – Glossary
vii. Annex 6 – Acronyms
viii. Annex 7 – Task Authorization Form;
ix. The Contractor's bid (referred hereinafter as the "Bid") which consist of the following:
   i. The Contractor's bid dated _____ (insert date of bid in any resulting contract), as amended _____(insert date(s) of amendment(s) if applicable in any resulting Contract), not including any software publisher license terms and conditions that may be included in the bid, not including any provisions in the bid with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of web link) in the bid;
   ii. The Contractor's bid clarification during the bid evaluation process dated _____ (insert date if bid clarification, as required, in any resulting contract);'' and
   iii. The Contractor's Usability Assessment dated _____ (insert date of Usability Assessment n any resulting contract).

7.18 Foreign Nationals (Canadian Contractor *OR* Foreign Contractor)

(*to be confirmed at contract award*)

SACC Manual clause A2000C *(*2006-06-16*)* Foreign Nationals (Canadian Contractor)

OR

SACC Manual clause A2001C *(*2006-06-16*)* Foreign Nationals (Foreign Contractor)

7.19 Insurance Requirements

The following clauses, inserted by reference, form part of this Contract:

SACC Manual clauses G1005C (2008-05-12)

7.20 Limitation of Liability

7.20.1 This section applies despite any other provision of the Contract and replaces the section of the 2035 General Conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this section, even if it has been made aware of the potential for those damages.

7.20.2 First Party Liability:

a. The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the contract that relate to:

   i. any infringement of intellectual property rights to the extent the Contractor breaches the section of the general conditions entitled "Intellectual Property Infringement and Royalties";

   ii. physical injury, including death.

b. The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

c. Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

d. The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (a) above.

e. The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

   i. any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including Applicable Taxes) for the goods and services affected by the breach of warranty; and

ii. any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of 0.75 times the total estimated cost (meaning the dollar amount shown on the first page of the contract in the block titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1,000,000.

In any case, the total liability of the Contractor under paragraph (e) will not exceed the total estimated cost (as defined above) for the contract or $1,000,000, whichever is more.

f. If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

7.20.3 Third Party Claims:

a. Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

b. If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite paragraph (a), with respect to special, indirect, and consequential damages of third parties covered by this section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

c. The Parties are only liable to one another for damages to third parties to the extent described in this paragraph 7.20.3.

7.21 Ownership

7.21.1 Canada acknowledges that ownership of the EPS belongs to the Contractor or its licensor and is not transferred to Canada. As a result, any reference in the contract to any part of EPS as a deliverable must be interpreted as a reference to the license to access and use the EPS, not to own the EPS.

7.21.2 Canada acknowledges that, in performing any warranty, maintenance, support and professional services related to the EPS (if required under the Contract), the Contractor and its employees, agents, and subcontractors may develop and share with Canada ideas, know-how, teaching techniques and other intellectual property. Unless otherwise provided in the Contract, ownership to that intellectual property will remain with the Contractor. As long as the Contractor at all times observes the confidentiality provisions of the Contract, the Contractor will be entitled to use that intellectual property for whatever purposes it sees fit, including in the services it provides to its other customers, on the condition that Canada also has the right to use that intellectual property for its own business purposes at no additional cost. The Contractor agrees that all data, know-how or other intellectual property created or owned by Canada will remain the property of Canada, regardless of whether that data is created, processed, or stored using the EPS.

7.22 EPS Documentation

7.22.1 Copyright in the EPS Documentation will not be owned by or transferred to Canada. However, Canada has the right to use the EPS Documentation and may, for its own internal purposes, copy it for use by individuals using or supporting the EPS, as long as Canada includes any copyright and/or proprietary right notice that was part of the original document in any copy. Unless provided otherwise in the Contract, Canada must not otherwise reproduce the EPS Documentation without first obtaining the written consent of the Contractor.

7.22.2 The Contractor guarantees that the EPS Documentation contains enough detail to permit an Administrator to access, test and use all features of the EPS.

7.22.3 The Contractor must deliver the EPS Documentation in Canadian English. If the EPS Documentation is available in both of the two official languages of Canada, the Contractor must deliver it in both Canadian French and Canadian English. If the EPS Documentation is only available in Canadian English, it may be delivered in that language; however, Canada then has the right to translate it. Canada owns any translation and is under no obligation to provide it to the Contractor. Canada will include any copyright and/or proprietary right notice that was part of the original document in any translation. The Contractor is not responsible for technical errors that arise as a result of any translation made by Canada.

7.22.4 At no additional cost to Canada, the Contractor must update the EPS Documentation throughout the Period of the Contract, and any extension thereof, to the most current release level consistent with the EPS delivered under the Contract. The Contractor must provide these updates to Canada within ten (10) days of the update being available. These updates must include supporting documentation for all modifications to the EPS, including new versions and new releases that Canada is entitled to receive under the contract and must identify any problems resolved, enhancements made, or features added to the EPS, together with access instructions

7.23 Service Rights

7.23.1 The Contractor must obtain and maintain all necessary intellectual property rights and grants required to deliver the services under the Contract. The Contractor also guarantees that all necessary consents to that grant have been obtained. Canada agrees that its only remedy and the Contractor's entire obligations in relation to a breach of this guarantee are the remedies and obligations set out in the section entitled "Intellectual Property Infringement and Royalties" contained in the 2035 General Conditions.

7.23.2 The Parties agree that only the conditions that expressly form part of the Contract by being written out in full in the Articles of Agreement or listed in the Priority of Documents section in the Articles of Agreement form part of the Contract. Any conditions accompanying or enclosed with the EPS if any, do not form part of the Contract and, therefore, are not part of Canada's license and do not affect the rights of the Parties in any way. The Contractor agrees that in no event will Canada or any Client or User be required to enter into any additional license agreement with respect to the EPS or any portion of it. The Contractor acknowledges that any additional license agreement relating to the EPS signed by anyone other than the Contracting Authority is void and of no effect.

7.24 Changes in Functionality

a. During the Term of the Contract, the Contractor must continue to deliver the EPS as described in the Contract and Contractor's bid. Where the Contractor has reduced or eliminated functionality in the EPS, Canada, at Canada's sole discretion, will:

    i. have, in addition to any other rights and remedies under this contract or at law, the right to immediately terminate this Contract and be entitled to a refund of any advanced payment;

b. If the Contractor removes any functions from the EPS and offers those functions in any new or other services, the Contractor agrees to provide to Canada as part of Canada's License, the part of those new or other services which contain the relevant functions, or the whole programs to the extent that the relevant functions cannot run separately, pursuant to the same terms and conditions of this Contract.

c. Where Contractor increases functionality in the EPS, such functionality must be provided to Canada without any increase in the EPS cost.

7.25 EPS Warranty, Maintenance and Support Services

The following is in accordance with Annex 1 – Statement of Work (SOW)

7.25.1 EPS Warranty:

The Contractor warrants and represents that the EPS will meet or exceed all of the Specifications set out in the contract and SOW during the entire Term of the Contract.

7.25.2 EPS Maintenance:

a. The Contractor must continue to maintain and upgrade the EPS as commercial EOS (i.e. the Contractor or the software publisher must be continuing to develop new code in respect of the EPS to maintain its functionality, enhance it, and deal with Errors) for the entire Term of the Contract. After that time, if the Contractor or the software publisher decides to discontinue or no longer maintain the EPS, the Contractor must provide written notice to Canada at least 12 months in advance of the discontinuation;

b. The Contractor must ensure that, as a minimum, the EPS works with Microsoft Internet Explorer 11, including compatibility mode; and

c. The Contractor must ensure that the MWS works with all future commercially available versions of Microsoft Internet Explorer (version 11) and 2 previous versions (version 11 - 2). This requirement is in effect as of Microsoft Internet Explorer 11.

7.26 No Suspension of Services

The Contractor must not suspend any part of the Services where (a) Canada is reasonably disputing any amount due to Contractor; or, (b) any unpaid but undisputed amount due to Contractor is less than ninety (90) business days in arrears.

7.27 Contractor Use of Canada's Data

The Contractor is provided a limited license, for the Term of the Contract, to Canada's Data for the sole and exclusive purpose of providing the Work, including a license to collect, process, store, generate, and display Canada Data only to the extent necessary in the providing of the Services.

The Contractor must:

a. keep and maintain Canada's Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss;

b. use and disclose Canada's Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with the Contract and applicable law; and,

c. not use, sell, rent, transfer, distribute, or otherwise disclose or make available Canada's Data for the Contractor's own purposes or for the benefit of anyone other than Canada without Canada's prior written consent.

7.28 Loss of Data

In the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of Canada's Data or the physical, technical, administrative, or organizational safeguards put in place by the Contractor that relate to the protection of the security, confidentiality, or integrity of Canada's Data, the Contractor must, as applicable:

a. notify Canada as soon as possible, but no later than twenty-four (24) hours of becoming aware of such occurrence;
b. cooperate with Canada in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by Canada;
c. perform or take any other actions required to comply with applicable law as a result of the occurrence;
d. indemnify, defend, and hold harmless Canada for any and all Claims (as defined herein), including reasonable attorneys' fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from Canada in connection with the occurrence;
e. be responsible for recreating lost Data in the manner and on the schedule set by Canada without charge to Canada; and,
f. provide to Canada a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence.

7.29 Data Privacy and Information Security

Without limiting the Contractor's obligation of confidentiality as further described herein, the Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to:

a. ensure the security and confidentiality of Canada's Data;
b. protect against any anticipated threats or hazards to the security or integrity of Canada's Data;
c. protect against unauthorized disclosure, access to, or use of Canada's Data;
d. ensure the proper disposal of Canada's Data; and,
e. ensure that all employees, agents, and subcontractors of the Contractor, if any, comply with all of the foregoing. Representations and Warranties

The Contractor made statements regarding its experience and expertise in its bid that resulted in the award of the Contract. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract. The Contractor also represents and warrants that it has, and all its resources and subcontractors that perform the Work have, and at all times during the contract Period they will have, the skills, qualifications, expertise and experience necessary to perform and manage the Work in accordance with the Contract, and that the Contractor (and any resources or subcontractors it uses) has previously performed similar services for other customers.

7.30 Dispute Resolution

7.30.1 Interpretation

a. "dispute" means any disagreement regarding any issue identified by the Contractor in the notice submitted to Canada in accordance with subparagraph 3.b., and includes any claim by the Contractor arising from such disagreement and any counterclaim by Canada, but does not include any claim by either party for punitive or exemplary damages, property damages, insured losses, injury to persons, death, or any claim based on an allegation of libel or slander; and

b. The dispute resolution procedures set out herein, do not apply to any claim by Canada against the Contractor, except any counterclaim in a dispute as defined in subparagraph 7.30.1.a.

7.30.2 Consultation and Co-operation

The parties agree to maintain open and honest communication throughout the performance of the Contract. The parties agree to consult and co-operate with each other in the furtherance of the Work and the resolution of problems or differences that may arise.

7.30.3 Notice of Dispute

a. Subject to subparagraph 7.30.1.a., any dispute between the parties to the Contract of any nature arising out of or in connection with the Contract which could result in a claim by the Contractor, and which is not settled by consultation and co-operation, must be resolved in the first instance by Canada, whose written decision or direction will be final and binding subject only to the provisions herein. Such written decision or direction includes, but is not limited to, any written decision or direction by Canada under any provision of the Contract.

b. The Contractor shall be deemed to have accepted the decision or direction of Canada referred to in subparagraph 7.30.3.a. above and to have expressly waived and released Canada from any claim in respect of the particular matter dealt with in that decision or direction unless, within 15 working days after receipt of the decision or direction, the Contractor submits to Canada a written notice of dispute requesting formal negotiation under paragraph 7.30.4. Negotiation. Such notice must refer specifically to paragraph 7.30.4. Negotiation, and must specify the issues in contention and the relevant provisions of the Contract.

c. The giving of a written notice in accordance with subparagraph 3.b. above does not relieve the Contractor from complying with the decision or direction that is the subject of the dispute. Such compliance, however, must not be construed as an admission by the Contractor of the correctness of such decision or direction.

d. If a dispute is not resolved promptly, Canada must give such instructions as, in Canada's opinion, are necessary for the proper performance of the Work and to prevent delays pending a resolution of the matter. Unless Canada terminates the Contract, orders the Contractor to suspend the Work, or takes the Work out of the hands of the Contractor, the Contractor must continue to perform the Work in accordance with the provisions and requirements of the Contract and the instructions of Canada. Such performance will not prejudice any claim that the Contractor may have with respect to the matter in dispute.

e. Nothing in these Dispute Resolution procedures relieves the Contractor from its obligation to provide any other notice required by the Contract within the time specified in the Contract.

7.30.4 Negotiation

a. Within 10 working days after receipt by Canada of a notice referred to in paragraph 7.30.3. Notice of Dispute, the parties must commence negotiations in order to resolve the dispute. Negotiations must occur initially between representatives of the Contractor and Canada who play a direct supervisory role in the performance, administration or management of the matter in dispute under the Contract.

b. If the representatives referred to in subparagraph 7.30.4.a. above are unable to resolve some or all of the issues which are the subject of the negotiations within 30 working days, the parties must refer the remaining issues which are in dispute to a second level of negotiation between a principal or principals of the Contractor and a higher ranked representative or representatives of Canada.

c. If negotiations fail to resolve the dispute within 30 working days from the date of the dispute is referred to the second level of negotiation, either party may, by giving written notice to the other party, within 15 working days from the end of such period, request that mediation be undertaken to assist the parties to reach agreement on the outstanding issues.

d. Additional levels of negotiation and periods of time longer than those prescribed above, may be agreed to in writing, by the parties. At each level of negotiation, both the Contractor and Canada must identify their representative(s).

e. Should the abovementioned notice provisions not be adhered to, the dispute will be considered to be abandoned.

7.30.5 Mediation

a. If mediation is requested in accordance with paragraph 7.30.4. Negotiation, mediation must be conducted in accordance with paragraph 7.30.8. Rules for Mediation of Disputes.

b. If a Project Mediator has not previously been appointed for the purposes of the Contract, a Project Mediator must be appointed in accordance with paragraph 7.30.8. Rules for Mediation of Disputes, forthwith after delivery of a notice in accordance with paragraph 7.30.4. Negotiation, requesting mediation.

c. If the dispute has not been resolved within
   i. 30 working days following the appointment of a Project Mediator in accordance with 7.30.5.b., if a Project Mediator was not previously appointed;
   ii. 30 working days following receipt by Canada of a responding party's written notice referred to in 7.30.3., "Notice of Dispute", if a Project Mediator was previously appointed; or
   iii. such other longer period as may have been agreed to by the parties;

the Project Mediator must terminate the mediation by giving written notice to the parties stating the effective date of termination.

7.30.6 Confidentiality

All information exchanged during alternative dispute resolution procedures, by whatever means, must be without prejudice and must be treated as confidential by the parties and their representatives, unless otherwise required by law. However, evidence that is independently admissible or discoverable must not be rendered inadmissible or non-discoverable by virtue of its use during an alternative dispute resolution process.

7.30.7 Settlement

Any agreement to settle all or any part of a dispute, by whatever means, must be in writing and be signed by the parties or their authorized representatives.

7.30.8 Rules for Mediation of Disputes

7.30.8.1 Appointment of Project Mediator

a. The parties to the Contract may, by mutual consent, at any time after entry into the Contract, appoint a mediator (the "Project Mediator") to conduct mediation proceedings in accordance with these Rules for Mediation of Disputes, in regard to any dispute that may arise with regard to the interpretation, application or administration of the Contract. In this case, they must jointly enter into a contract with the appointed Project Mediator.

b. If the parties do not appoint a Project Mediator pursuant to subparagraph 7.30.8.1.a., the parties must appoint a Project Mediator within 30 days following receipt of a written notice from either party, requesting that mediated negotiations be undertaken in accordance with these Rules to assist the parties to reach agreement on any outstanding issues that may be in dispute. Any contract entered into with the appointed Project Mediator must meet the requirements as set out for the contract described in paragraph a. of subparagraph 7.30.8.1.a.

c. When mediation is requested pursuant to subparagraph 7.30.8.1.a., the parties must within 15 days send to the Project Mediator
   i. a copy of the notice requesting negotiation under paragraph 7.30.3. Notice of Dispute;
   ii. a copy of Canada's written position in relation to the notice, the issues in contention and the relevant provisions of the contract; and
   iii. a copy of the Contractor's written request for mediation required under paragraph 7.30.4. Negotiation.

d. If the parties have not agreed on a Project Mediator, Canada must forthwith provide the Contractor with a list of 3 candidates from which the Contractor shall choose the Project Mediator

e. If the parties have not previously entered into a contract with a mutually acceptable Project Mediator, a contract and a Mediation Agreement must be negotiated forthwith, which must

incorporate or otherwise comply with the provisions of these Rules and be in the form attached to this agreement as paragraph 7.30.9.Mediation Agreement. If negotiations are unsuccessful, or if for other reason the individual is unwilling or unable to enter into a contract to act as Project Mediator, the parties must repeat the process with the Contractor's second selected mediator.

f. Upon execution of the contract with the Project Mediator the parties must provide the Project Mediator with copies of the documents referred to in subparagraph 7.30.8.1.c.

7.30.8.2 Confidentiality

a. Subject to subparagraph 7.30.8.2.b., and unless otherwise agreed in writing by the parties, the Project Mediator, the parties and their counsel or representatives must keep confidential all matters and documents disclosed during mediation proceedings except where the disclosure is necessary for any implementation of any agreement reached or is required by law.

b. Evidence that is independently admissible or discoverable in any arbitral or judicial proceeding must not be rendered inadmissible or non-discoverable by virtue of its use in mediation proceedings.

c. Neither party must make transcripts, minutes or other records of a mediation conference.

d. The personal notes and written opinions of the Project Mediator made in relation to mediation are in the Project Mediator's sole possession and control, are confidential, and may not be used in any subsequent proceeding between the parties or where they are opposed in interest without the express written permission of the parties.

e. All information exchanged during mediation procedures, by whatever means, must be without prejudice and must be treated as confidential by the parties and their representatives, unless otherwise required by law.

7.30.8.3 Time and Place of Mediation

The Project Mediator, in consultation with the parties must set the date, time and place of any mediation conference as soon as possible, bearing in mind that, subject to agreement to the contrary between the parties, only 30 working days are available within which to attempt to settle the dispute.

7.30.8.4 Representation

a. Representatives of the parties may be accompanied at the mediation conference by legal counsel or any other person.

b. If the Project Mediator is a lawyer, the Project Mediator must not provide legal advice to a party during the course of the mediation conference, but may recommend that a party obtain independent legal advice before finalizing a settlement agreement.

7.30.8.5 Procedure

a. The parties agree to an exchange of all facts, information and documents upon which they intend to rely in any oral or written presentation during the mediation. This exchange must be completed no later than three working days prior to the date set for a mediation conference.

b. The Project Mediator must be free to meet with the parties individually during a mediation conference if the Project Mediator is of the opinion that this may improve the chances of a mediated settlement, and either party may request such an individual meeting at any time.

c. The parties may agree to extend the 30 working days available for settlement of the dispute through mediation, and the Project Mediator must record that agreement in writing.

7.30.8.6 Settlement Agreement

a. The parties must record in writing any settlement agreement reached, with sufficient detail to ensure a clear understanding of

   i. the issues resolved;
   ii. any obligations assumed by each party including criteria to determine if and when these obligations have been met; and
   iii. the consequences of failure to comply with the agreement reached.

b. The parties agree to carry out the terms of a settlement agreement as soon as possible and, in any event, within any time periods specified in the agreement.

7.30.8.7 Termination of Mediation

a. Either party may withdraw from mediation at any time without reason and, in that event, the Project Mediator must give each party a written notice terminating the mediation and establishing the effective date of termination.

b. If, in the opinion of the Project Mediator, either party fails to mediate in good faith or fails to comply with the terms of these Rules, or if the Project Mediator, at any time during mediation, is of the opinion that further negotiations will fail to resolve the issues outstanding, the Project Mediator may terminate the negotiations by providing the parties with a written notice of termination, stating therein the Project Mediator's reasons for the termination, and the effective date of termination.

c. If a dispute has not been resolved within 30 working days or such other longer period as may have been agreed to by the parties, the Project Mediator must terminate the mediation by giving written notice to the parties stating the effective date of termination.

7.30.8.8 Costs

The parties agree that they will each be responsible for the costs of their own representatives and advisors and associated travel and living expenses. Fees and expenses of the Project Mediator and all administrative costs of mediation, such as the cost of the meeting room(s), if any, must be borne equally by the parties.

7.30.8.9 Subsequent Proceedings

a. The parties must not rely on or introduce as evidence in any arbitral or judicial proceeding, whether or not such proceeding relates to the subject matter of mediation,
   i. any documents of other parties that are not otherwise producible in those proceedings;
   ii. any views expressed or suggestions made by any party in respect of a possible settlement of issues;
   iii. any admission made by any party in the course of mediation unless otherwise stipulated by the admitting party; and
   iv. the fact that any party has indicated a willingness to make or accept a proposal or recommendation for settlement.

b. The Project Mediator must neither represent nor testify on behalf of either of the parties in any subsequent investigation, action or proceeding relating to the issues in mediation proceedings.

c. The Project Mediator must not be subpoenaed to give evidence relating to
   i. the Project Mediator's role in mediation;
   ii. or the matters or issues in mediation, in any subsequent investigation, action or proceeding and the parties agree to vigorously oppose any effort to have the Mediator so subpoenaed.

7.30.9 Mediation Agreement

An agreement to submit an existing dispute to mediation will be embodied in the following agreement:

a) **Agreement to Submit:** We, the undersigned parties, agree to submit the controversy regarding [DESCRIBE BRIEFLY] to mediation.

b) **Location:** The mediation shall be held in a mutually agreed upon location.

c) **Discovery:** The parties agree to prepare mediation briefs for the mediator outlining their positions and exchange all information upon which they intend to rely in any oral or written presentation during the mediation. This exchange shall be completed no later than three days prior to the date set for the mediation.

d) **Cost:** The parties agree that they will each be responsible for the costs of their own legal counsel and personal travel. Fees and expenses of the mediator and all administrative costs of the mediation, such as the cost of the hearing room, if any, shall be borne equally by the parties.

e) **Schedule:** The parties shall jointly select a date for the mediation that is no later than [___] days from the date a mediator is selected and the matter is to be concluded within [___] days, subject to any extension recommended by the mediator and agreed to by the parties.

f) **Termination of Agreement**: Either party may terminate this agreement at any time during the mediation.

g) **Confidentiality:** All Information exchanged during the entire procedure shall be regarded as "without Prejudice" communications for the purpose of settlement negotiations and shall be treated as confidential by the parties and their representatives, unless otherwise required by law. However, evidence that is independently admissible or discoverable shall not be rendered inadmissible or non-discoverable by virtue of its use during the mediation.

h) **Caucusing:** The mediator is free to caucus with the parties individually, as he sees fit to improve the chances of a mediated settlement. Any confidential information revealed to the mediator by one party during such caucusing may only be disclosed to the other party(ies) with the former party's express permission.

i) **Prohibition against Future Assistance:** It is agreed that the mediator will neither represent nor testify on behalf of any of the parties in any subsequent legal proceeding between the parties or where they are opposed in interest. It is further agreed that the personal notes and written opinions of the mediator made in relation to this mediation are confidential and may not be used in any subsequent proceeding between the parties or where they are opposed in interest.

7.31 Joint Venture Contractor

***(Note to Bidders**: At the time of award this clause will be deleted if the Contractor is not a joint venture. If the Contractor is a joint venture, the necessary information will be filled in. If there are specific provisions that apply to each of the members, rather than to the JV contractor as a whole, appropriate wording will be added to sub-article (f). If the contract is being awarded to a joint venture contractor, all the members of the JV may be asked to sign the contract.*)

a. The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members: [*list all the joint venture members named in the Contractor's original bid*].

b. With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:

i. _____ has been appointed as the "representative member" of the joint venture Contractor and has fully authority to act as agent for each member regarding all matters relating to the Contract;

ii. by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and

iii. all payments made by Canada to the representative member will act as a release by all the members.

c. All the members agree that Canada may terminate the contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.

d. All the members are jointly and severally or solitarily liable for the performance of the entire Contract.

e. The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

f. The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

Note to Bidders: *This Article will be deleted if the Bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

ANNEX 1

STATEMENT OF WORK

TABLE OF CONTENTS

List of Figures

List of Tables

PART 1: CANADA'S E-PROCUREMENT SOLUTION OVERVIEW

This overview provides a high level overview of the Government of Canada (GC) procurement environment, and the business outcomes being sought through the e-Procurement Solution (EPS).

1.1 STRUCTURE OF THIS DOCUMENT

This document consists of two sections:

1. Section I, Statement of Objectives, provides introductory material on the EPS business model. It is intended to provide context for the requirements detailed in the Statement of Requirements. The following briefly describes the content of Parts 1:

    a. **Part 1: Canada's E-Procurement Solution** Overview provides information on the procurement itself and a high level overview of the procurement environment;

2. Section II, Statement of Requirements, consisting of five sections, provides information on requirements:

    a. **Part 2: Legislative, Regulatory and Policy Requirements:** provides a list of applicable legislation, policies, directives and guidelines for the GC.

    b. **Part 3: Non-Functional Requirements:** identifies cross-cutting, high level outcomes that are applicable across all functions and services.

    c. **Part 4: Technical Requirements:** provides technical requirements for the solution.

    d. **Part 5: Functional Requirements:** provides functional requirements broken down by section that outlines each functional area of the procurement process. Each functional area description identifies the requirements for which the Contractor is responsible and provides the foundation for specific Contractor outcomes and deliverables.

    e. **Part 6: Management and Oversight Requirements**: describes the elements that are required in order for the Contractor to conduct a successful transition to administering the EPS and a successful phase-out and transition to subsequent Contract.

1.1.1 RACI Framework

Throughout this document, the RACI Framework is leveraged to set forth the roles and responsibilities of the Contractor and GC for the set of common services and processes that apply to the provision, delivery and management of all services in support of GC's EPS initiative.

Table 1 - Definition of RACI Model

Activity/Role	Description

R – Responsible	Those who do the work to achieve the task. Responsible for action/implementation. Responsibility can be shared as delegated by the Approving Authority.
A – Accountable	Approver or final Approving Authority for reviewing, approving work before it is implemented.
C – Consulted	Those whose opinions are sought; and with whom there is two-way communication.
I – Informed	Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

1.2 COMMON TERMINOLOGY

Key terms and acronyms used throughout this document may be found in Annex 5 & 6: Glossary and Acronyms.

1.3 SCOPE OF THE WORK

The Contractor must deliver, enable, support, manage and assist in the application of a web-based e-Procurement Solution. The Contractor must ensure mature transformation, change management methodologies, tools and processes, including necessary training and communications with management, partners and end users. The Contractor must operate a fully hosted and supported web-based e-Procurement Solution that takes a modern and flexible approach to administering public procurement from the point of process initiation (normally associated with needs identification) through the strategic sourcing and procurement lifecycle to close of the Contract. The Contractor must deliver these and related services in both of Canada's official languages to clients within Canada and abroad.

This procurement will establish a government wide standard for procurement.

1.3.1 Potential Future Scope

In addition to policy and legislative changes, the Contractor must ensure that changes to future requirements with respect to technology, financial management, privacy, security and the extension of services to other jurisdictions are implemented.

1.4 LEGISLATIVE AND POLICY REQUIREMENTS

Public procurement activities conducted by GC are governed by a number of acts, including those for international and national trade agreements, as well as policies, directives, and guidelines provided by the Treasury Board Secretariat (TBS) or Public Works and Government Services Canada (PWGSC). A non-exhaustive list of all relevant federal and provincial legislation, regulations and policies that must be followed is included in Part 2: Legislative, Regulatory and Policy Requirements. This list is subject to change during the term of the Contract.

The service will be further governed by broader legislation, regulations, and policies to which the Contractor must adhere, including technical standards and specifications. Ensuring the security and protection of personal information remains a priority for the GC and all solutions and processes must adhere to all relevant legislation including but not limited to those related to privacy and the handling and storage of personal information.

1.5 FEDERAL PROCUREMENT OVERVIEW

1.5.1 GC Procurement and Responsibilities

PWGSC is GC's common service provider for acquisitions services. It is responsible for providing a broad range of procurement solutions to support the delivery of government programs and services.

PWGSC's acquisitions services are mandatory for most federal government entities above certain delegated thresholds, generally $25K for goods and $2M for services. However, PWGSC establishes methods of supply which allow clients to acquire higher values of goods and services when utilizing those instruments. Under TBS Policy, there are currently ten commodities for which clients are required to use those instruments regardless of value. In addition, some entities such as Canada Revenue Agency have specific contracting authorities that make PWGSC's services optional for their procurement or have special authorities related to their organization's mandate (e.g. Shared Services Canada for software and hardware for workplace technology devices and the Department of National Defence for the procurement of defence supplies).

1.5.2 Acquisitions Program Overview

The Acquisitions Program (AP), delivered by PWGSC's Acquisitions Branch (AB) and regional offices (including Washington and Koblenz), is the GC's primary procurement service provider.

On average, the GC processes over 475,000 procurement transactions valued at $17B annually from which PWGSC AP processes 50,000 transactions valued at $14B annually. Currently, the value of GC procurement for commercial goods and services conducted by AP clients under their own delegations or against PWGSC Framework Agreements is approximately $4B annually, or 20-25% of the total contract spend and 75-80% of procurement transactions. The remainder of the GC contract spend includes commercial goods and services procured by PWGSC on behalf of clients, as well as complex contracts for construction, major military, space, information and equipment systems, and major services such as property management services and other outsourced services.

The AP delivers its mandated role and services through the following sub-programs of services: General Procurement Services; Customized Procurement Services; Acquisitions Stewardship; and Acquisitions Support and Innovation.

- **General Procurement Services** PWGSC is the GC's primary procurement service provider offering a broad base of standard or unique procurement solutions including contracts, standing offers, supply arrangements and procurement tools. The role of PWGSC in this area is to manage contracts for goods and services on behalf of client departments and agencies of the GC and includes the management of contractual activities such as planning, acquisitions and contract

administration. In general, while the procurement solutions addressed in this sub-program can be complex, they are typically the common, frequently purchased requirements of most departments.

- **Customized Procurement Services** PWGSC is the GC's procurement provider for customized procurement solutions including industry consultations, market surveys, conducting complex competitive solicitations and contract negotiations, award and management of contracts including legal agreements. Often such procurements include a wide range of technically complex systems and services, are unique, high in dollar value and are long-term agreements. Because of the complexity and the nature of the requirement [the procurement of goods and/or services] they usually require early involvement of AP procurement specialists in the definition phase of the requirement and require dedicated procurement teams in the implementation phase of the procurement strategies. Since these procurements may be sensitive in nature and/or require a multi-phased approach, risk management, performance management, financial management and change management are all important aspects of the overall project management regime.

- **Acquisitions Stewardship** PWGSC is the GC's primary steward of government acquisitions providing the federal government and suppliers with a well-functioning acquisitions system. As such, PWGSC ensures effective management of the acquisitions function by: providing direction and guidance to stakeholders; overseeing the development and deployment of government-wide strategies, designing processes and tools to preserve the integrity of the acquisitions system; and maintaining the system's relevance and focus on the evolving needs and resource realities of federal departments and agencies, and the capacities of supplier communities.

- **Acquisitions Support and Innovation** PWGSC is the GC's primary provider of common services and programs for the federal government, industry and consumers that support or leverage the acquisitions function: from the provision of standards development and conformity assessment services to the disposal of government goods, as well as programs that use the acquisitions system to advance the government's socio-economic objectives for Canadians.

1.5.3 Volumetric

Due to the limitations of the legacy systems currently in place, the volumetric data in this attachment are based on limited statistical information and is provided for information purposes only.

- **Commodities:** Approximately 5,000 Good and Service Identification Number (GSIN) classification codes are in use by the AP. GC procurements are currently classified using GSIN coding, United Nations Standard Products and Services Code (UNSPSC) coding will be implemented as the classification scheme for EPS.

- **Contracts and Amendments:** GC Business Volume and Value.

Figure 1 - GC Business Volume and Value

		PWGSC-AB PROCUREMENT ACTIVITY *3yr Average (FY10/11 - FY12/13)*		OGD PROCUREMENT ACTIVITY *(CY2012)*		TOTAL GOVERMENT PROCUREMENT ACTIVITY	
Type of Transaction		#Transactions	Value	#Transactions	Value	#Transactions	Value
Commodity Management	SA	609	*Value Excluded*			609	*Value Excluded*
	SA Amendments	918				918	
	SO	4,958				4,958	
	SO Amendments	11,196				11,196	
Contract Management	Contract	13,924	$7.347B	228,254	$2.670B	242,178	$10.017B
	Contract Amendments	15,764	$4.129B	34,512	$0.352B	50,276	$4.480B
	Call-Ups	3,266	$0.451B	144,138	$1.668B	147,404	$2.119B
	Call-Up Amendments	0	$0.000B	18,129	$0.064B	18,129	$0.064B
Total		50,635	$11.927B	425,033	$4.754B	475,668	$16.688

- **Framework Agreements:** On a yearly basis, PWGSC manages nearly 10,000 supply arrangements and standing offers. These standing offers and supply arrangements represent multi-supplier awards under approximately 2,000 Framework agreements.

- **GC User Base:** There are approximately 3,500 purchasing employees responsible for sourcing and contracting activities in the GC. PWGSC and Shared Services Canada (SSC) are the largest employer (40%), followed by Department of National Defence (DND) (25%) and all other departments (35%). In addition, over 60,000 users providing administrative services within the GC order goods and services off PWGSC Framework Agreements and initiate unique procurements. The EPS will also potentially be used by others, such as the general public, and must not be restricted to a limited number of users or to a specific group of users.

- **Document, Templates and Forms:** Currently, there are over 200 separate documents, templates and forms used in AP's processes.

- **Supplier Base:** PWGSC maintains 25,000 unique supplier records.

1.6 E-PROCUREMENT STRATEGIC CONTEXT

1.6.1 Problem Statement

PWGSC's AP and the broader GC procurement environment are hampered by complex manual-intensive processes, a lack of standardized procurement processes and associated master data, a fragmented legacy infrastructure of over 40 "outdated" information technology application systems, and limited capabilities for spend management and strategic sourcing. At the same time, the current procurement environment presents challenges for the ongoing financial and workforce sustainability of PWGSC's AP.

1.6.2 Opportunity Statement

An EPS provides significant opportunities to transform and modernize both the AP and the overall GC acquisitions function.

Introducing an enabling technology that will automate and standardize processes will allow the AP to shift from a focus on manually carrying out transactional procurement, to strategic sourcing of

customized/complex procurement. This shift will be facilitated by the introduction of online self-serve tools to process standard transactions. By doing so, this allows Acquisitions' employees to contribute their expertise to more strategic and complex activities.

In addition, there is a further opportunity to transform the process for suppliers to do business with GC by renewing GC's Government Electronic Tendering Service and providing innovative services such as electronic bidding to lower barriers for suppliers.

Public procurement supports GC operations by ensuring the timely delivery of the goods and services needed to deliver on operational mandates and deliver value to citizens and further supports the private sector by ensuring free, open, and transparent access to government opportunities.

1.6.3 Core Functionalities/Uses

The EPS will provide functionalities to support a number of Business Areas and at the core of the solution will be the following procurement functions:

- **e-Cataloguing** – will provide a structured, searchable repository of information on the goods and services offered by pre-qualified Suppliers, in the form of various e-Catalogues, to allow GC client users to determine whether required item(s) are available for selection, and to initiate and complete Orders from the applicable e-Catalogue. This functionality will also include the ability to create and maintain e-Catalogues as well as provide for the management of established e-Catalogues and resulting Orders; together with ability to manage the associated Framework Agreements (Methods of Supply) with Suppliers which inform each e-Catalogue's structure and contents.

- **e-Sourcing / CLM** – where the goods or services required by a Procuring Entity are not available within an existing e-Catalogue or where the terms and conditions of the e-Catalogue's associated Method of Supply are such that a second-stage procurement is required among the pre-qualified Suppliers to provide the good and/or service; e-Sourcing will provide the functionality for GC users to initiate a Sourcing Event (RFx) to seek offers, evaluate and qualify one or more Supplier(s) to provide the required good and/or service.

- Underpinning each of these main functional Business Areas is the Order/Contract creation/management functionality which will allow GC users to establish the resulting agreement(s) with qualified Supplier(s); either for inclusion in an existing e-Catalogue, creation of a new e-Catalogue or as a one-off Order/Contract. Details about these operations can be found in the introduction of the e-cataloguing and e/sourcing/CLM section under Part 5.The list of functional requirements outlined in Part 5 are:

    - GENERAL
    - PORTAL
    - SOURCING AND CONTRACT MANAGEMENT
    - PROCUREMENT MANAGEMENT
    - SERVICE PROCUREMENT MANAGEMENT

- FINANCIAL MANAGEMENT
- BUSINESS INTELLIGENCE
- SUPPLIER RELATIONSHIP MANAGEMENT
- DATA AND INFORMATION MANAGEMENT
- USER MANAGEMENT

1.6.4 Electronic Vision

Canadians want and expect ease of access to information and services. Canadians also expect service solutions to include technology based components such as electronic identity validation, electronic transactions including documentation and signatures, in a safe and secure manner. Further, Canadians want to interact in real time, using a wide range of platforms including mobile technology.

EPS must respond to these expectations by making the best possible use of available technology while ensuring stewardship of taxpayers' funds.

The goals of the project are to:

- achieve better value for Canadians through improved procurement outcomes;
- improve client service by providing easy, web-based access to procurement information and services to Departments and Agencies;
- provide easy, web-based access to information and services that reduce Supplier's burden of participating in the procurement process;
- achieve an integrated approach to the management of government spend; and
- enable procurement professionals with new tools, technology and processes to deliver effective client services.

1.6.5 Business Outcomes and Objectives

Key Performance Indicators (KPIs) will be used to help track progress towards project goals. The following table presents the KPIs for the EPS project, organized by the Business Goals with which they are aligned and may be modified in consultation with the Contractor upon Contract award. Within each grouping, the KPIs are presented by key stakeholder groups and planned outcomes for that group. While the Contractor's performance is not expected to be tied directly to these KPIs, they are indicators of successful adoption and outcomes.

Figure 2 - Business Outcomes and Objectives

Business Goal	Stakeholders & Planned Outcomes	Key Performance Indicator (and Objective)
1. Achieve better value for Canadians through improved procurement outcomes.		
	Stakeholder: **Canadians:** ***Includes the entire Canadian general population***	
	Outcome: Increased visibility and transparency on GC contractual spend	• % of GC spend available as Open Contract Data (% increase year-over-year) • Increase in level of detail of Open Contract Data (increase year-over-year)
2. Provide easy, web-based access to procurement information and services to Departments and Agencies		
	Stakeholder: **Departments and Agencies (Our Clients)**	
	Outcome: Empowered individual procuring entities through self-service tools	• % of Catalogues e-enabled. (% increase year-over-year)
	Outcome: Greater access to procurement information	• % of spend under management – GC procurement transactions completed through PWGSC procurement instruments. (% increase year-over-year)
	Outcome: Streamlined client service delivery and reduced process burden	• Time to contract award from requisition receipt. (% decrease year-over-year)
	Outcome: Enhanced value through increased competition	• Average price of items in GC price index. (% decrease year-over-year)
3. Provide easy, web-based access to information and services that reduce the burdens of participating in the procurement process		
	Stakeholder: **Industry (Our Suppliers):** ***Includes all suppliers providing goods and services to the Government of Canada.***	
	Outcome: Simplified and faster processes	• Time to contract award from requisition receipt. (% decrease year-over-year)
	Outcome: Easier, more functional technology to simplify and reduce costs of finding and bidding on opportunities	• % of bids received electronically (% increase year-over-year) • Number of unsuccessful procurement processes (% decrease year-over-year)
	Outcome: maintaining access for suppliers of all sizes	• % volume contracts awarded to SMEs (% increase year-over-year)
	Outcome: Increased consistency in the use of Framework Agreements	• % of spend under management – GC procurement transactions completed through PWGSC procurement instruments. (% increase year-over-year)

Business Goal	Stakeholders & Planned Outcomes	Key Performance Indicator (and Objective)
4. Achieve an integrated approach to the management of government spend		
	Stakeholder: **The Government of Canada:** ***Includes all branches of the Canadian federal government***	
	Outcome: Enable greater process efficiencies and reduced cost to support procurement infrastructure	• Time to contract award from requisition receipt (% decrease year-over-year)
	Outcome: Improved capture and quality of raw data to support effective decision-making	• % of GC spend flowing through EPS (% increase year-over-year)
	Outcome: Greening government operations	• % of bids received electronically (% increase year-over-year) • % of requisitions received electronically (% increase year-over-year)
5. Enable Procurement Professionals with new tools, technology and processes to deliver effective client services.		
	Stakeholder: **AP Procurement Professionals:** ***Includes all supply professionals within the Acquisitions Program***	
	Outcome: Improved employee productivity and satisfaction through streamlined and efficient digital tools	• PWGSC contract value per AP employee (% increase year-over-year) • Cost per $100 PWGSC contract value (% decrease year-over-year) • Employee satisfaction survey (increasingly positive results)
	Outcome: Improved quality of data captured throughout procurement process	• % of contracts issued using EPS (% increase year-over-year) • % of Catalogues e-enabled (% increase year-over-year) • % of GC spend flowing through EPS (% increase year-over-year)
	Outcome: Reduction of process burdens through a paperless work environment	• Time to contract award from requisition receipt. (% decrease year-over-year) • % of requisitions received electronically (% increase year-over-year) • % of bids received electronically (% increase year-over-year)
	Outcome: Enhanced capacity for complex procurement	• Reduction of full time employees assigned to low dollar value procurement (% decrease year-over-year)

Business Goal	Stakeholders & Planned Outcomes	Key Performance Indicator (and Objective)
		• Increase of full time employees assigned to complex procurements. (% increase year-over-year)

1.6.6 Stakeholders (User Communities)

Technology is an important aspect of modern business, and stakeholders tend to be familiar and comfortable with working and communicating electronically. The GC is responding, and has been steadily working towards increasing its on-line service offerings through web-enabled initiatives, including BuyandSell.gc.ca, and upgrades to meet or exceed the current GC web accessibility standards.

The following describes procurement's key stakeholder groups. Collectively these stakeholder groups' needs and requirements emphasize the need for an AP enabled by an EPS.

1.6.6.1 Canadians

The entire Canadian general population requires visibility into where their taxpayers' dollars are spent and experience better value through improved procurement outcomes. They demand increased visibility and transparency on GC contractual spend stewardship to increase their confidence in public servants' ability to fulfill their duties and to make informed procurement decisions. The EPS will provide Canadians with up to date information regarding procurement activities.

1.6.6.2 The Government of Canada Departments and Agencies

All branches of the Canadian federal government require an integrated approach to the management of government spend. The near-elimination of paper-based processes will Green government operations.

The EPS will provide all Departments, Crown corporations and agencies, as identified in Schedules I, I.1, II, III, IV and V of the Financial Administration Act with acquisitions requirements access to information and services that improve procurement outcomes through self-service tools, facilitate greater access to procurement information, streamline client service delivery and reduce process burden with 24/7 access to self-managed tools with automated processes and to enhance value through increased competition.

1.6.6.3 Other Levels of Government

Provinces and territories along with the broader public sector require an aligned approach across governments to enable greater process efficiencies and reduce cost to support procurement infrastructure and improve the capture and quality of raw data to support effective decision-making and greater visibility into spend information.

1.6.6.4 Procurement Professionals

The EPS will allow all supply and procurement professionals new tools, technology and processes to deliver effective client services to be able to improve the productivity and satisfaction, improve the quality of data captured throughout the procurement process, reduce the process burdens through a paperless work environment and increase quality control and decrease the amount of risk in the procurement process.

- Procurement professionals from inside of Public Works and Government Services Canada (PWGSC) – Acquisition Program (AP) – will serve as the shared services procurement provider for the GC to assist Clients in undertaking the procurement process, managing contracts, and establishing and maintaining procurement standards and broader strategic instruments.

- Procurement professionals from outside PWGSC-AP will use EPS to identify the availability of particular goods and services to meet their requirements; and to select item(s) and place Orders directly through the e-Catalogue or to initiate a Sourcing Event via a Requisition.

1.6.6.5 Suppliers

All suppliers providing goods and services to the GC require access to information and services that reduce the burdens of participating in the procurement process. The GC is committed to provide simplified and faster procurement processes with greater consistency and with more two way dialogue. This will enable easier, more functional technology to simplify and reduce the costs of finding and bidding on opportunities. It will also provide more transparency and substantiated decision-making to balance large procurements and maintaining access for suppliers of all sizes and in all parts of Canada. This will also simplify the process for Framework Agreements to increase consistency in their use across government.

Suppliers to the GC – will use the EPS to respond electronically to requests and Orders for goods and services (via the e-Catalogue) to respond electronically or manually to Sourcing Events (RFx); and to update their e-Catalogue offerings and maintain their supplier profile and information within the EPS.

1.7 PRIORITIES FOR THE CONTRACTOR

The EPS project provides an opportunity to implement an electronic based, client-centric approach and improve service delivery to all stakeholders (procurement professionals, suppliers and the public) in a cost effective and efficient manner. Recent and ongoing advances in both technology and business processing methodologies are vital factors which will enable high-level procurement objectives / principles to be met.

The Contractor must provide a responsive and dynamic service delivery model that:

- utilizes a client-centric, modern, technologically advanced solution to ensure client satisfaction by providing clients and stakeholders with user-friendly access to services through online delivery channels and using streamlined paperless processes;
- ensures communication channels reflect ongoing client expectations, and enables easy access to information for clients, stakeholders and service delivery partners to allow informed decision making;

- maintains financial stewardship through measurable cost-efficiency and cost-effectiveness in the administration of the service, and contains a transparent cost structure supported by monitoring and oversight (reporting and validation);
- has a flexible, adaptable technology solution (including software and hardware) to accommodate changes in a timely and cost-efficient manner (policy changes, process changes, partnerships);
- maximizes the administrative efficiency of the business model using streamlined processes, with automation where possible across all delivery partners and in alignment with other government initiatives where feasible;
- ensures the design of a robust, reliable system with appropriate backups to support business continuity;
- ensures that security and privacy standards are met across all business lines (such as call centre and information management, incident tracking and breach management); and
- minimizes potential incidences of fraud by having the necessary controls and authentication tools in place.

PART 2: LEGISLATIVE, REGULATORY AND POLICY REQUIREMENTS

2.1 INTRODUCTION

The automated services delivered though the EPS must facilitate GC's compliance with all its acts, regulations, guidelines and policies, as detailed below.

Legislation, regulations, policy, directives, standards and guidelines provide further useful information to determine the compliance requirements of the EPS and of the delivery of services to GC, as well as the scope and complexity of the business workflow and functional requirements that must be implemented. While the current location of the latest electronic version of each document is provided, all are subject to change and the EPS must facilitate GC's continued compliance with all legislative, regulatory and policy requirements.

Where possible, Part 4 Technical Requirements and Part 5 Functional Requirements will identify the relevant or applicable legislation, regulations, policy, directives, standards and guidelines associated with a requirement within each Section.

2.2 FEDERAL ACTS AND REGULATIONS

The automated services delivered though the EPS must facilitate GC's compliance with all its policies, directives and guidelines, regardless of whether or not more specific references appear in Part 4 and Part 5, including but not limited to:

Access to Information Act

The Privacy Act

Personal Information Protection and Electronic Documents Act (PIPEDA)

Library and Archives of Canada Act

Official Languages Act

Canadian Payments Act

Electronic Payments Regulations

All other federal Acts, including those not listed above, can be found in their entirety on the Department of Justice website *www.justice.gc.ca*.

2.3 FEDERAL POLICIES, DIRECTIVES STANDARDS AND GUIDELINES

The Contractor and EPS must comply directly with all relevant federal policies, directives and guidelines, including but not limited to:

Policy Framework for Information and Technology

Policy on Information Management

Policy on Management of Information Technology

Operational Security Standard: Management of Information Technology Security (MITS)

Policy on Privacy Protection

Policy on Access to Information

Directive on the Administration of the Access to Information Act

Policy on Government Security

Operational Security Standard on Physical Security

Policy on Financial Management Governance

Policy on Internal Audit

Communications Policy of the Government of Canada

Federal Identity Program Policy

Directive on Identity Management

Guideline on Defining Authentication Requirements

Policy on Acceptable Network and Device Use

Policies, Standards and Directives governing on-line service delivery, including but not limited to: (These web standards replace *Common Look and Feel 2.0* (CLF 2.0)

Web Standards for the Government of Canada

Standard on Web Accessibility

Standard on Web Usability

Standard on Privacy and Web Analytics

Standard on Web Interoperability

Standard on Email Management

Standard on Optimizing Websites and Applications for Mobile Devices

Additional policies, standards, guidelines and directives can be found in their entirety on the *Treasury Board Secretariat of Canada website*.

2.4 PROCUREMENT POLICIES, ACTS, STANDARDS, DIRECTIVES, REGULATIONS AND AGREEMENTS

The automated services delivered though the EPS must facilitate GC's compliance with all its policies, acts, standards, directives, regulations and agreements, regardless of whether or not more specific references appear in Part 4 and Part 5, including but not limited to:

Comprehensive Land Claim Agreements

Procurement Strategy for Aboriginal Business (PSAB)

Canada's Free Trade Agreements

Agreement on Internal Trade

Industrial Security

PWGSC Integrity Framework

Data Standard on Classification of Procurement Items

Directive on the Application of the Goods and Services Tax/Harmonized Sales Tax

Directive on the Payment, Collection and Remittance of Provincial Taxes and Fees

Directive on Privacy Requests and Correction of Personal Information

Directive on Privacy Practices

National Joint Council Travel Directive

Security and Contracting Management Standard

PWGSC Supply Manual

Standard on Vendor Record

Procurement Strategy for Aboriginal Business: Guidelines for Buyers/Government Officials

Retention Guidelines for Common Administrative Records of the Government of Canada

Sources of Federal Government and Employee Information 2009, Index of Standard Personal Information Banks

Canadian International Trade Tribunal Act.

Policy on Green Procurement

Procurement Review Policy

Canadian Content Policy

Contracting Policy

Policy on Title to Intellectual Property Arising Under Crown Procurement Contracts

Policy Notices and TB Circulars - Contracting

Contracting Policy Notice 2007-04 - Non-Competitive Contracting

Common Services Policy

Employment Equity Policy

Government Contracts Regulations

Procurement Ombudsman Regulations

Department Public Works and Government Services Act

Financial Administration Act

2.5 COMMITMENT TO SECURITY AND PRIVACY OF PERSONAL INFORMATION

GC has one of the most comprehensive privacy legislative and policy frameworks in the world. The privacy of Canadians is protected by the *Canadian Charter of Rights and Freedoms* through various provisions, but especially in Section 8 of the Charter, which provides: "Everyone has the right to be secure against unreasonable search or seizure." The *Criminal Code* has various provisions creating criminal offences relating to invasions of privacy, and in particular, Part VI of the Code, which relates to the interception of private communications.

Many federal statutes contain provisions limiting the use and disclosure of personal information collected by specific federal government institutions to specified purposes including the *DESD Act Part 4 Protection of Personal Information*.

The *Privacy Act* places limits on the collection, use and disclosure of personal information by federal government institutions. It also gives Canadians the right to access and correct personal information about them that is held by institutions. More information on Security and Privacy will be included with Annex 2

Further, from an IT Security perspective, when applicable to the EPS requirements, the Contractor must comply with the following:

IT Security Guidance

ITSG-41 Security Requirements for Wireless Local Area Networks

ITSG-33 IT Security Risk Management: A Lifecycle Approach

ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones

ITSG-31 User Authentication Guidance for IT Systems

ITSG-04 Threat and Risk Assessment Working Guide has been replaced by the Harmonized Threat And Risk Assessment Methodology (TRA)

ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada

PART 3: NON-FUNCTIONAL REQUIREMENTS

3.1 CONTEXT

The purpose of this section is to identify cross-cutting, high level outcomes or requirements that are applicable across all aspects of the EPS.

3.2 HIGH LEVEL COMMITMENTS

3.2.1 Ability to Adapt to Change

The EPS must be able to adapt to change and accommodate change requests from the GC on an agreed to timeline. GC anticipates that the following possible types of changes are likely to occur within the life of the Contract**:**

- adding a new or modifying an existing workflow to accommodate new policies or approaches in the procurement process (such as the introduction of integrity measures), including administrative rules such as maximum allowable purchasing limits, conditions for being eligible to buy and/or sell goods and services, and effects on the business rules caused by other variables;
- introducing new communications messages and/or materials within existing client channels, addressing new administrative requirements in messaging to clients and new messaging timeframes;
- entering into new information sharing and/or electronic data exchanges with new or existing systems or services (i.e. new information feeds into the supplier relationship management environment); and
- modifying policies and administrative requirements related to individual procurements (i.e. authorities, actions required by clients); all of which will involve changing work flow, organization and administrative procedures.

While GC anticipates that there may be change management costs for resources and activities related to modifying the flexible and configurable EPS, the information technology capacity required of the Contractor as described in Part 4 Technical Requirements clearly lays out requirements for a flexible solution that is able to evolve over time without incurring significant information technology change management costs.

3.2.2 Solution Flexibility

As stated earlier, one of the EPS objectives is to simplify and streamline business processing wherever possible, while at the same time maintaining the flexibility to modify processes to address new program requirements or circumstantial events that might limit normal business processing without hindering ease of use for all clients.

The Contractor must also have the ability to manually intervene, when authorized or directed by the Project Authority, into automated solutions or develop workarounds to modify or suspend standard procurement operations. In such cases, the Contractor must:

- document process changes;
- maintain complete records of accounts impacted by the change; and
- develop ad-hoc reports to quantify and qualify changes as a result of the modified or suspended processing.

3.2.2.1 Accommodating Policy Driven Changes

Changes to the procurement environment, policies and processes are frequent. Related Federal programs also improve processing efficiencies within their internal systems, and through streamlining their own business processes. The EPS must be flexible enough to adapt to these changes and modify the activities, processes, and configurations accordingly, often with short turnaround times.

3.2.2.2 Accommodating Changes in Technical Environment

The EPS is expected to be built on a flexible architecture such as the Service Oriented Architecture (SOA) concept which allows an open, interoperable and flexible systems environment. The EPS must fit in to the GC technology environment without forcing changes to GC technology stack and desktop environment.

The overall solution must also be flexible and adaptable enough to integrate and interoperate with existing and/or new systems within GC by supporting electronic information exchanges with other systems using protocols, format, contents and transfer timing that meets GC's standards and business needs.

There is a possibility that changes to the technical environment may occur and the Contractor must make continuous improvements to meet its performance targets within its solution domain and to maintain interoperability with other technology contact points throughout the Contract period.

3.2.3 Solution Usability

The user interface needs to be easy to learn how to use and easy to remember how to use. Ensuring a high level of satisfaction for the user experience is a key business objective and must be a top priority for the Contractor.

To ensure successful adoption of the EPS by users, the Contractor must deliver intuitive, user-centric systems and services that are selected, designed, configured, and implemented with the user experience in mind. The Contractor must further adopt and leverage best practices in solution design, such as but not limited to:

- Ensure consistent and standardized user interface in the EPS.
- Guide the users by providing context sensitive help messages and visual process maps available when requested by GC.
- Intuitive user interface design by adhering to best practices in web, such as "Make interactive Objects obvious", "Give Feedback", "Never have users repeat anything", "Always have default values in fields and forms", etc.

- Incorporating best practice web application usability tools and plug-ins, such as Mouse-over details, Auto-Complete/Suggest, Calendar Scheduler, Multi-select combo box, Date Picker, Drag and Drop manager, Hot-Keys, etc.
- Smooth integration with productivity tools and desktop environment, such as drag and drop capability with MS Office products suite.
- Allow a user to create hyperlinks to any document so that it can be referenced anywhere within the solution.
- Allow a user to personalize and manage their own views. This includes, but not limited to creating favorites, short-cuts, setting default actions, and default values for business processes and data.
- Protect a user from system and human errors, by putting automatic system based fault-tolerance features such as auto-save of the work in progress and by putting confirmation steps in user workflows.

3.2.4 Government Requirements and Solution Design

The GC may stipulate requirements unique to government administration that are beyond those of non-public sector business practices including security, privacy, and official languages requirements. Some streamlining opportunities may not be possible due to these requirements.

3.2.5 Principles of Effective Information Management

Information Management is an integral part of the Contractor's responsibilities. KPI's and transactional Data allows the AP to measure and report on performance, create new procurement policies, make strategic purchasing decisions, gauge supplier performance, release open data as a matter of public transparency, and maintain high quality client service at all stages of the procurement lifecycle.

The Contractor must apply the basic principles of effective information management to:

- avoid unnecessary collection of duplicate information, reconcile inconsistencies and ensure data quality;
- ensure that information is complete, accurate, current, relevant, and understandable;
- support access to information subject to policy and legal requirements;
- prevent unlawful access to information; and
- safeguard information against loss, theft and damage.

Managing EPS information and data requires adherence to Government of Canada legislation, policies, and procedures, including the *Policy on Government Security*, *Access to Information Act, Privacy Act, Privacy Regulations, Official Languages Act, Library and Archives of Canada Act,* and *Public Works and Government Services Canada Act*.

The above mentioned legislation, as well as those applicable policies referenced within this SOW dictates the specific management of information requirements, including the following:

- what and how information is to be captured and used;

- how long a program or service will operate; and
- how long the information will be needed for operational and legal / evidential purposes.

A retention and disposal policy for EPS information must follow the *Policy on Information Management*.

3.3 SERVICE DELIVERY IN BOTH OFFICIAL LANGUAGES

As required by the *Official Languages Act*, the GC has an obligation to provide service delivery in Canada's two official languages: English and French. When designing the solution and ongoing client contact channels, the Contractor must:

- Provide materials for any user in both official languages. Personal communications to clients must be provided in the user's language of choice, with English as the default language if the client has not indicated a preference.
- maintain a record of user's language preference so that all personal communications are received in their language of choice.
- ensure that all client-oriented communication materials are available for distribution in both official languages.
- be available in the official language of choice. This includes all user-facing information and tools such as background text, web applications, error and warning messages, system tables, system generated messaging, and any print and on-line documentation.

3.4 OFFICIAL LANGUAGES OBLIGATIONS FOR PROCUREMENT

When procurements are national in scope or originate from an office having the obligation to serve the public in both official languages, pursuant to Acts and Regulations, all regular or standardized documents must be provided in both official languages. As such, users must be able to produce and make available procurement material (including, but not limited to public notices, terms and conditions, forms, bid solicitations, standards, purchase descriptions, catalogues and contracts) in either both Official Languages.

Additionally:

- All public solicitations must be bilingual. Users must be able to create and publish English and French solicitation (RFx) documents using EPS.
- The EPS must keep both language versions of the solicitation under the same solicitation identification and process.
- During bid solicitations, the question and answer process must include the publication of the supplier's question and the response in both official languages.
- GC Users must be capable of searching and buying in both official languages - meaning catalogues must be capable of being created with attributes in both official languages for the same product.

3.5 SECURITY AND PRIVACY

3.5.1 Personal and Protected information

The Contractor has an ongoing responsibility for personal and protected information, including, but not limited to, the following:

- Supplier identification information (e.g. names, addresses, company profiles, résumés, work experience, previous contracts completed, and clients).
- Supplier financial data (e.g. banking information).
- Procedures, forms, computer systems and data file layouts, and Internet Web sites, etc.

Contact information (including business name), biographical information, educational information, financial information, evaluations/assessments, Social Insurance Number (SIN), other identification number (e.g. Business Number) and signature.
Annex 2 – Security and Privacy will provide a table of security requirements and the Security Requirements Traceability Matrix.

The Contractor in accordance with Annex 2 – Security and Privacy, must:

- be responsible for the safekeeping, protection and privacy of this information, and upon close-out of the Contract, returning all information to Canada;
- ensure that the conversion, imaging and subsequent destruction of any personal information originating from the Contract is conducted in accordance with all applicable legislation and policies; and
- safeguard any information created, destroyed, stored, accessed and modified in the delivery of the solution in accordance with legislated requirements. In doing so, the EPS must:
- ensure that the quality, accuracy, completeness and integrity of the data within the system is always maintained through the use of appropriate validation measures;
- ensure that the consistency of the data is both reconcilable and auditable;
- maintain a multi-channel history of information sent or received, information exchanged, and account updates performed by or on behalf of the client;
- protect sensitive information and safeguard against theft, including identity theft or unauthorized third parties acting on behalf of clients, fraud or disclosure as per the *Privacy Act* and *the Department of Employment and Social Development Act, Part 4 Protection of Personal Information*; and
- ensure any destruction of records is completed following the standards set out in the *Library and Archives Act* and EPS Disposition Authority.

3.6 COMMUNICATIONS

There is an expectation, as identified in the objectives, that the EPS must prioritize electronic, e-enabled online and self-service formats of communication. However, taking into account the national nature and overall complexity of the relationships with the clients, the EPS must also offer multiple service delivery channels including call centre, IVR, e-mail, message centre, and client service portal.

Regardless of the channels selected by clients for account management and communications, the Contractor must integrate client contact and service delivery channels so that the same information "set" is modified, updated, and accessed consistently. There is an overall expectation that the Contractor must apply, to the greatest extent possible, the principle of first contact resolution to client services across all delivery channels.

While high-level service delivery channel requirements are described below, all service delivery channels must also meet approved security and privacy requirements (legislative and policy). The Contractor, within the confines of the principles stated in Section.2 must develop processes and products to support proactive communication with users. Communications must address key messages throughout the life cycle, including initial communication and reminders of users' obligations. The objectives are to ensure that users are fully informed of their obligations and options during every stage of the procurement lifecycle and to facilitate ongoing interaction with users to help them effectively manage their procurements.

3.6.1 Communications Development Principles

The Contractor must develop an overall EPS communications plan, including user messaging, for Project Authority approval. The communication plan will be expected to provide a link between business objectives and communications planning and delivery; explain how communications will support the project objectives and which strategic choices have been taken and why; build common understanding of audiences and priorities; create continuity in communications activity over an extended period; articulate objectives and measures of success; and explore and mitigate communications risks. The Project Authority will approve the communications plan and make any required changes to targeted user communications.

The Project Authority will review and approve all standard (web-based and hard copy when required) forms and user messaging for online and phone use (e.g. scripts for phone calls and e-chats) prior to implementing these communications materials. While GC must undergo internal approvals for the authority to use communications messages, once approval is confirmed, the content must be implemented in a timely manner as part of ongoing operations. The Contractor must employ a solution approach that allows for seamless and transparent communications content changes so that messaging can be modified within work flows or client channels when required (e.g. use of a content management system component).

The Contractor must provide GC with the ability to generate custom communications through EPS to users as required. The Contractor must ensure that GC has the ability to access a repository of pre-approved communications messages and standard communications templates to generate these communications to users through EPS.

Table 2 – Communication Development Principles

Principle	**Reason**

Transformational approach	Facilitates empowering opportunities for individuals to contribute to the shared values, mission and objectives enabling cultural change.
Consultative and open	Supports a transparent approach and stakeholder engagement with the project.
Credibility	A credible communication approach engenders the community towards a belief that the end goal is achievable.
To involve not just inform	Supports a transformational approach and stakeholder engagement with the project.
Face-to-face communication	Facilitates involvement and feedback.
Avoid information 'overload'	Accurate and timely information is essential.
Consistent messages	Consistency enhances the professionalism and credibility of the project.
Repeat messages and vary mechanisms	The more ways a message can be communicated, the more likely it is to be internalised. Using different mechanisms ensures repetition without individuals 'switching off' and has more chance to reach a wider audience.
Respond to information demand: Encourage team to seek the kind of information stakeholders need.	Ensures engagement with the change.
Tailor communication to audience needs	Makes information 'real' to the audience. The audience is more likely to listen if the information is pertinent to their current frame of reference.
Central co-ordination	Ensures consistent approach.
Manage expectations	Encourages audience to believe in what you to tell them. Need to be realistic not overly optimistic.
Listen and act on feedback	Encourages support in the approach by being responsive to the needs of the audience. Ensures approach meets changing audience needs.

3.6.2 Online Service Delivery

The Contractor must adhere to the relevant IT policies, directives, and legislation as detailed in Part 2 including Policies, Standards and Directives governing on-line service delivery.

The GC is committed to providing accessible online information and services to the public and to maintaining trust and confidence in GC websites. The Contractor must meet GC web directives for accessibility and web standards throughout the duration of the Contract. While the list of policies and directives to be followed is available in Part 2, a formal approval process, including applicable testing and audits must be incorporated into the overall governance structure to ensure policy compliance.

3.7 SERVICE DESK

3.7.1 Service Manager

The Contractor must provide a service manager to meet with GC's representatives during Business Days from 08:00 to 17:00 ET and be reachable using communication methods as approved by GC, 24 hours per day, 7 days per week, 365 days per year, for Management Services escalation (Incidents, Change Requests), high Priority and Security Incidents, Service Level reviews, release implementation activities, release maintenance and release window scheduling, service quality, and service reporting.

3.7.2 Call Center

While the program is focused on e-enabled service delivery, the Contractor must provide and maintain a secure service desk accessible by users to provide support in the use of EPS and to resolve users' technical challenges.

The service desk must provide toll-free telephone number(s) for clients, automated routing, and tools that monitor call response time, successful call completion, and unresolved calls. The Contractor must support the receipt of international calls by providing appropriate toll-free phone numbers for international callers.

Unresolved problems raised by clients in the Contractor's service desk including for example, those subject to policy interpretation or processing exceptions must be escalated to an authority designated by GC for direct resolution or decision-making.

3.7.3 Service Desk Requirements

The objective of the EPS Service Desk is to support the agreed IT service provision by performing various supporting activities such as:

3.7.3.1 General Responsibilities

- act as a first point of contact for all user incidents, requests and general communication;
- restore 'normal service operation' as quickly as possible in the case of disruption;

- improve user awareness of IT issues and to promote appropriate use of IT services and resources; and
- assist other IT functions by managing user communication and escalating incidents and requests using defined procedures.

3.7.3.2 Infrastructure Incidents

- Hardware
- System software
- Network response time

3.7.3.3 Application Incidents and "How To" support

- EPS
- GC's business applications

3.7.3.4 Password Support

- Resets
- Requests for account privilege change requests
- Requests for End User account activation, suspension and termination

3.7.3.5 Service Requests

- Installs, Moves, Adds, and Changes requests

3.7.3.6 Escalation to Subject Matter Experts (SME)

- route incidents relating to a particular procurement policy or process to the appropriate SME resource.

The Contractor must provide a Service Desk that is accessible as per table 3.7.3.8 Service Desk Tiers and Response Levels in all Canadian time zones using service delivery channels such as but not limited to:

- **Phone:** Providing a phone line allowing clients to speak directly with service desk support agents to submit and resolve service requests.
- **Interactive Voice Response (IVR):** Develop and implement the secure Interactive Voice Response (IVR) service channel. The IVR should provide general information to clients who do not choose to self-identify. This service should present clients with an appropriate array of self-service options. IVR scripts will fall under the umbrella of those communications products requiring approval, but the Contractor must ensure the channel is responsive and facilitates the exchange of information. The IVR service must be provided in both official languages 24 hours a day, 7 days a week. Clients must have the option of speaking to a service desk support agent at any point during the operating hours.
- **Email:** Providing an e-mail address allowing clients to use their email program to submit service requests. The client receives confirmation and notifications via e-mail.

- **Live Chat:** Providing a chat session, allowing clients to open a text dialogue with service desk support agents
- **Self Service:** Providing clients the ability to create service request and attempt self-resolution via accessing a knowledge base. Clients can also access their existing tickets and track the status of all their requests
- **Persons with Disabilities:** The GC is committed to providing broad-based services, ensuring public accessibility and increasing public awareness of issues affecting persons with visual, auditory, mobility and cognitive impairments. In accordance with GC policies on Accessibility and Usability, the Contractor must provide alternative formats for all client-oriented communications and services to clients (e.g. TTY, TTD keypads, IVR, audio tapes, large print, Braille, and electronic versions of all forms) as required. A TTY line must be provided at all times. The Contractor must ensure that service desk technology is updated and incorporated into the overall client services, as necessary and in accordance with the Standards and policies identified in Part 2.
- **Frequently Asked Questions:** Allows both service desk support agents and clients to reference a list of common questions and answers that can leverage a knowledge base.

3.7.3.7 Tiered Service Desk Support – User Segmentation

Table 3 - Service User Segmentation: Application by User Type

	Procurement Professionals (supply professionals within the GC)	Industry (all suppliers providing goods and services to the GC)	Departments and Agencies (End Users accessing procurement information and services)	VIPs (DMs, ADMs, EPS GC Project Team)
E-Catalogs	Tier 2 - Gold	Tier 2 - Gold	Tier 3 - Silver	VIP
Contract Management Solution	Tier 1 - Platinum	Tier 2 - Gold	Tier 3 - Silver	VIP
Supplier Relationship Management	Tier 2 - Gold	Tier 2 - Gold	Tier 2 - Gold	VIP
Sourcing Management	Tier 1 - Platinum	Tier 1 - Platinum	Tier 3 - Silver	VIP
Business Intelligence	Tier 3 - Silver	Tier 3 - Silver	Tier 3 - Silver	VIP

3.7.3.8 Service Desk Tiers and Response Levels

Table 4 - Service Desk Tiers and Response Levels

Tier	Support Hours	Priority Level	Incident Acceptance Response Time(1)	Incident Resolution Time(2)
Tier 1 **Platinum** **Premium**	Mon-Fri 06.00-19.00 Sat-Sun 08.00-17.00	(1) Urgent	≤15 elapsed minutes	≤ 1 elapsed hours
		(2) High	≤15 elapsed minutes	≤ 4 elapsed hours
		(3) Medium	≤ 2 Standard Operating Hours	≤ 24 Standard Operating Hours
		(4) Low	≤ 4 Standard Operating Hours	≤ 48 Standard Operating Hours
Tier 2 **Gold** **Enhanced**	Mon-Fri 06.00-19.00 Sat-Sun 08.00-17.00	(1) Urgent	Not supported under Tier 2	
		(2) High	≤30 elapsed minutes	≤ 4 elapsed hours
		(3) Medium	≤ 4 Standard Operating Hours	≤ 24 Standard Operating Hours
		(4) Low	≤ 6 Standard Operating Hours	≤ 48 Standard Operating Hours
Tier 3 **Silver** **Basic**	Mon-Fri 06.00-19.00	(1) Urgent	Not supported under Tier 3	
		(2) High		
		(3) Medium	≤ 4 Standard Operating Hours	≤ 24 Standard Operating Hours
		(4) Low	≤ 6 Standard Operating Hours	≤ 48 Standard Operating Hours
VIP Tier	24/7	(1) Urgent	≤15 elapsed minutes (assumes process available)	≤ 2 elapsed hours (assumes process available)
		(2) High		
		(3) Medium		
		(4) Low		

Incident Acceptance Response Time: Parameter to measure the time for the Service Desk to accept (i.e., receive, log and assign for Resolution) an Incident. Time is measured from the time the Incident is received by the Service Desk agent to the time it is logged and assigned for Resolution in the ITSM System.

Incident Resolution Time: Parameter to measure the time by which the Contractor resolves any Incident from the time the Incident is received by the Service Desk, by any method. Time is measured from the time of Incident receipt by the Service Desk to the time the Service Desk agent logs the Resolution in the ITSM System.

3.7.3.9 Priority Levels

Table 5 - Priority Levels

Priority Level 1: Emergency/Urgent – Critical Business Impact	The incident has caused a complete and immediate work stoppage affecting a critical function or critical infrastructure component, and a primary business process or a broad group of users (an entire department, floor, branch, line of business, or external user). No workaround available. Examples: ■ Major application problem (e.g., cataloguing, sourcing, call center, etc.) ■ Severe disruption during critical periods (e.g., fiscal year end processing ■ WAN or LAN outage ■ Security violation
Priority Level 2: High – Major Business Impact	A business process is affected in such a way that business functions are severely degraded, multiple users are impacted, a key authorized user is affected, or a critical function is operating a significantly reduced capacity or functionality. A workaround may be available, but is not easily sustainable. Examples: ■ Major data/database or application problem (e.g., exchange) ■ Email system is performing slowly, but workload is manageable ■ Security incursion on a non-critical system
Priority Level 3: Medium – Moderate Business Impact	A business process is affected in such a way that certain functions are unavailable to End Users or a system and/or service is degraded. A workaround may be available. Examples: ■ Telecommunication problem (e.g., BlackBerry, PBX digital/analog card) ■ End User device problem (e.g., hardware, software)

Priority Level 4: Low – Minimal Business Impact	An incident that has little impact on normal business processes and can be handled on a scheduled basis. A workaround is available or there is minimal negative impact on a user's ability to perform their normal daily work. Example: ■ "How to" questions ■ Service requests (e.g., system enhancement) ■ Peripheral problems (e.g., locally attached printer) ■ Preventative maintenance

3.7.3.10 General Roles and Responsibilities

The Contractor must provide all necessary resources and staff to operate the Service Desk. The Contractor must have support processes defined and practiced; including incident management, problem management, change management and escalation process. The Contractor must generate a service desk performance report and review it for adherence to service levels and performance metrics on an agreed schedule by GC.

Table 6 - General Roles and Responsibilities

General Roles and Responsibilities	Contractor	GC
Provide service desk support, help desk and material in both official languages.	R	A
Provide expert Level 1 [Level 2, and Level 3] assistance for inquiries about the features, functions and usage of hardware and software.	R	I
Identify, escalate (e.g., Level 2 and Level 3 escalation), manage Incident Resolution and Close Incidents and Service Requests, including those escalated to Third Parties.	R	I
Design and deploy a functional escalation model that provides for incident resolution. The EPS provide must escalate irresolvable incidents to another level of support for resolution and collect required information from the caller before escalation.	R	A
Provide appropriately trained Service Desk staff for Level 1 [and Level 2, and Level 3 if applicable] remote support to meet GC's requirements.	R	I
Coordinate the Root Cause Analysis process on recurring and Priority 1 and 2 Incidents.	R	I
Provide a closed-loop process for incident management, which includes informing the client of status changes or contacting the client for more information as required.	R	A

3.7.3.11 First Point of Contact Roles and Responsibilities

Table 7 - First Point of Contact Roles and Responsibilities

First Point of Contact Roles and Responsibilities	Contractor	GC
Recommend FPOC procedures.	R	C
Develop, document and maintain in the Standards and Procedures Guide FPOC Contractor procedures that meet GC's requirements and policies.	R	C

First Point of Contact Roles and Responsibilities	Contractor	GC
Review and approve FPOC procedures.	I	R
Select and implement software and hardware (e.g., Interactive voice response (IVR), ACD) needed to collect, track and manage Service Requests and Service Desk Incidents received by the Service Desk.	R	I
Provide FPOC call-in access via a toll-free number for all Service Desk Services described in this SOW and GC's Sites.	R	I
Provide FPOC and coordination for all Incident reports and requests for information and Service (e.g., IMACs) supported under this SOW.	R	I
Provide multiple alternative communications channels, including voice messages, email and intranet. In the case of Voice Communications Services, any IVR system must allow for immediate exit from the system and live communication with a Service Desk agent.	R	I
The IVR system must provide announcement and information support including the functionality to (a) Customize messaging; (b) Place emergency or response messages; and (c) Provide awareness messages relating to the services.	R	I
Record and redirect out-of-scope Incidents and Service Requests.	R	I

3.7.3.12 Operations and Administration

Table 8 - Operations and Administration Roles and Responsibilities

Operations and Administration Roles and Responsibilities	Contractor	GC
Define Service Desk Operations and Administration requirements and policies.	C	R
Develop, document and maintain in the Standards and Procedures Guide Service Desk Operations and Administration procedures that meet requirements and adhere to defined policies.	R	A
Review and approve Service Desk Operations and Administration procedures.	C	R
Provide additional Resources, as needed, during planned and unplanned critical events.	R	I
Track/manage/report Service Desk utilization.	R	I
Provide escalation contact list(s) for GC's contacts.	I	R
Maintain and provide escalation contact list(s) for all Service Tiers (including Third Parties such as vendors and service providers).	R	C
Issue broadcasts or other notices to provide status updates, as required, for planned and unplanned events.	R	C
Provide End User or manager online/portal access to Service Requests and Incident reports.	R	I
Develop and execute procedures for conducting End User Satisfaction surveys in accordance with the Service-Level Requirements.	R	I
Review and approve procedures for conducting End User Satisfaction surveys.	C	R
Maintain a continuous improvement program that improves Service Desk Service delivery.	R	A

Operations and Administration Roles and Responsibilities	Contractor	GC
Identify solutions that minimize the need to call the Service Desk (e.g., additional End User training, Self-Help Support opportunities, Root Cause Analysis).	R	C
Review and approve solutions that minimize the need to call the Service Desk.	I	R
Coordinate and make available environment documentation (i.e., Network configuration and inventory of software to be supported).	R	C

3.7.3.13 Request and Incident Management

The Contractor's Incident Management process must ensure the rapid restoration of Business and IT services following an unplanned deviation within the Contractor's Business and IT environments.

Request and Incident Management relate to the activities associated with end-to-end Incident Management processes, including escalation to Level 2 and Level 3 specialists through a defined process, including the Contractor's primary resources, Third Parties, such as hardware and software suppliers, other Third Party service providers as well as GC's internal technical support resources.

Table 9 - Request and Incident Management roles and Responsibilities

Request and Incident Management Roles and Responsibilities	Contractor	GC
Recommend Service Request and Incident Management procedures derived from the ITIL or ISO processes	R	C
Identify and describe priorities, response and Resolution targets for Incidents and Service Requests that have differing impacts.	I	R
Develop, document and maintain in the Standards and Procedures Guide Service Request and Incident Management procedures, including procedures to receive and respond to GC's Service Request Calls according to defined prioritization and Resolution targets that meet GC's requirements and policies.	R	A
Review and approve Service Request and Incident Management procedures.	I	R
Ensure that responses to Service Requests are based on priority and impact, rather than the method used to notify the Service Desk (e.g., by telephone, email, fax or direct input to Service Request system by End Users).	R	I
Provide a system to document, manage and track all Incidents, Service Requests, Incident reports and inquiries, regardless of the means by which the Service Requests are submitted (e.g., by telephone, email, fax or direct online input by End Users).	R	I
Provide an end-to-end Incident identification, escalation, Transfer, Resolution (management) and Closure process, including Incidents escalated to Third Parties.	R	I
Receive, track, answer and Resolve, or monitor to closure, End User and technical staff calls.	R	I

Request and Incident Management Roles and Responsibilities	Contractor	GC
Categorize, prioritize and log all Incidents (e.g., inquiries/problems/Service Requests) in the Service Desk Incident system.	R	I
Ensure that all incidents are identified by a unique number regardless of the contact method in order to make them traceable throughout the lifecycle of the service request.	R	I
Monitor Incidents (i.e., Service Desk Incidents) and escalate per policies and procedures until Resolution and End User satisfaction is achieved.	R	I
Troubleshoot Incidents using the Contractor's knowledge databases and/or Third Party knowledge databases (e.g., application Contractor knowledge databases).	R	I
Resolve Incidents at Level 1, if possible; otherwise escalate to appropriate Level 2 or 3 resources as required while collecting required information from the caller before escalation. Escalation of unresolved incidents to GC must only occur when all resolution options of the Contractor's functional escalation model have been exercised.	R	I
Prior to go-live, the Contractor must provide the escalation model it will apply, including the following information: (a) Number of tiers; (b) Description of tier escalation; (c) How escalations are handled; (d) Escalation reminders; (e) Escalation documentation; (f) Project Authority notification; and (g) Client status.	R	A
Provide expert functional and process "how to" assistance for in-scope applications at Level 1, and escalate to Level 2 or 3 resources as required.	R	I
Document solutions to Resolved Incidents in knowledge database.	R	I
Verify acceptance of Services by contacting the End User to confirm results and level of satisfaction.	R	I
Identify Incident characteristics and root cause for Level 1, [Level 2, and Level 3] Incidents.	R	C
Ensure that recurring Incidents that meet defined criteria are reviewed using Root Cause Analysis processes.	R	I
Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed/Resolved Service Requests	R	I
Provide authorization for Closing of Service Requests and Service Desk Incidents.	R	I
Send Service Requests and Service Desk Incident Closure notices per GC's policies.	R	I
Provide to GC complete and continuous access to all requests and incident closure information and data such as: (a) Incident receipt; (b) Incident identification; (c) Incident prioritization;	R	I

Request and Incident Management Roles and Responsibilities	Contractor	GC
(d) Incident management; (e) Incident assignment; (f) Incident logging, tracking and updating methods; and (g) Incident resolution and closing.		

3.7.3.14 End User Administration

Table 10 - End User Administration Roles and Responsibilities

End User Administration Roles and Responsibilities	Contractor	GC
Define requirements and policies regarding End User Administration.	C	R
Develop, document and maintain in the Standards and Procedures Guide End User Administration Contractor procedures that meet GC's requirements and policies.	R	C
Review and approve End User Administration procedures.	I	R
Receive track and process requests for End User account activation, changes and terminations.	R	I
Coordinate End User account administration, activation, changes and terminations (e.g., Password/account setup and Password Reset requests, remote access connectivity, email accounts, End User IDs).	R	I
Create, change and delete End User accounts per requests, in accordance with GC's security policies.	R	C
Coordinate, as necessary, with other specialized areas to manage End User accounts.	R	I
Perform or request Password Resets as required, in accordance with GC's security policies.	R	I

3.7.3.15 Self-Help Support

Table 11 - Self-Help Support Roles and Responsibilities

Self-Help Support Roles and Responsibilities	Contractor	GC
Define Self-Help Support requirements and policies.	C	R
Develop, document and maintain the Standards and Procedures Guide for Self-Help Support that adheres to GC's policies.	R	C
Review and approve Self-Help Support procedures.	I	R
Implement Self-Help Support capabilities that enable End Users to perform self-service, including Password Resets requests and other administrative functions, "how to" support through End User access to knowledge bases and online Incident status checking.	R	I
Provide Self-Help support in both Official Languages.	R	A
Monitor and review the effectiveness of Self-Help Support capabilities and usage.	I	R
Develop and provide recommendations for improvements to Self-Help Support capabilities.	R	A
Review and approve recommendations for improvements to Self-Help Support capabilities.	I	R

Self-Help Support Roles and Responsibilities	Contractor	GC
Implement approved recommendations for improvements to Self-Help Support capabilities.	R	I

3.7.3.16 Exception Requests

Table 12 - Exception Requests Roles and Responsibilities

Exception Requests Roles and Responsibilities	Contractor	GC
Define Exception Request policies and requirements.	I	R
Develop, document and maintain in the Standards and Procedures Guide Exception Requests process, procedures and required forms that meet GC's requirements and policies.	R	A
Review and approve Contractor Exception Requests procedures.	I	R
Document Exception Requests in Service Desk Incident management system, collect and analyze the request, recommend Exception Request action, process the request to fulfillment or denial, and advise the originator of the status.	R	I
Review and approve exception requests.	I	R
Take the necessary action to implement the request.	R	I
Provide Exception Request status to requestor, when approved.	R	I

3.7.3.17 Service Desk Reporting

Table 13 - Service Desk Reporting Roles and Responsibilities

Service Desk Reporting Roles and Responsibilities	Contractor	GC
Recommend a list of Service Desk management reports.	R	C
Review and approve list of Service Desk management reports.	I	R
Report on Service Desk statistics and trends as specified in the Standards and Procedures Guide (e.g., Service Request volumes and trends by types of End User).	R	I
Report on trends in Service Requests, and indicate any need for training.	R	I
Audit report results and Service Desk operations periodically.	I	R
Provide online/portal access to GC's Service Desk reports.	R	I

3.7.4 Service Standards

3.7.4.1 Performance Measurement and Reporting

A Performance Report must be provided to GC on an as-and-when-requested basis containing statistical information on the performance of the EPS as compared to the requirements set out in the "Service Level Objectives" Section.

The report must include the service request identifier, the service request status and information that the Project Authority requires to understand the service request and its resolution.

3.7.4.2 Service Standard Failures and Exclusions

With respect to Service Standard Failures or a negative trend towards failing to meet the Service Standards, upon conducting an analysis of the data captured as described in the "Performance Measurement and Reporting" Section, the Contractor must identify any discrepancies, including:

- Notify the Project Authority as soon as the Contractor becomes aware of such failure;
- Carry out a root cause analysis to investigate the underlying cause of the failure and preserve any data indicating the cause of the failure;
- Take action as agreed with the Project Authority to minimize the impact of the failure and prevent it from recurring;
- If practical, correct the failure immediately in order to resume fulfillment of the Service to the applicable Service Standard;
- Prepare and deliver to the Project Authority a report identifying the failure and, where possible, its cause, business impact, remedial plans, timeframe for implementing improvement plans, and any impact on the Services;
- Advise the Project Authority, as and to the extent requested by the Project Authority, of the status of all remedial efforts being undertaken by the Contractor with respect to the underlying cause of the failure.
- In calculating the Contractor's compliance with the Service Standards, events for which the root cause is outside the control of the Contractor must not be included in such calculations (unless the event is the result of acts or omissions of the Contractor):
- Any event arising as a direct consequence of an unforeseeable event; and
- Any action taken by the Contractor at the authorized request of the Project Authority contrary to the express, reasonable advice of the Contractor.

The Contractor must provide substantiation, where appropriate, that the root cause is outside its control to the Project Authority when requested.

3.7.4.3 Service Desk Availability

Table 14 - Service Desk Availability

SERVICE DESK AVAILABILITY			
Service Desk Availability	Service Measure	Performance Target	SLR Performance %
1) Automated Password Support 2) User Support 3) Supplier Support 4) IT Operations and Technical Support	Schedule	1) Sun.-Sat., 00.00-24.00 2) Mon.-Fri., 04.00-19.00 3) Sun.-Sat., 00.00-24.00	99.7%
	Formula	Availability (%) = 100% - Unavailability (%)	

SERVICE DESK AVAILABILITY		
		where Unavailability is defined as: (Σ Outage Duration × 100%) ÷ (Schedule Time - Planned Outage)
	Measurement Interval	First month: Measure daily Thereafter: Measure daily
	Reporting Period	First month: Report weekly Thereafter: Report monthly
	Measurement Method/Source Data	TBD

3.7.4.4 Phone Call Speed to Answer Response Time

Table 15 - Phone Call Speed to Answer Response Time

PHONE CALL SPEED TO ANSWER RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	≤ 20 seconds	≥ 90%
	Formula	[Number of phone calls to the Service Desk during the Measurement Interval that are answered within the Target Performance] divided by [total number of phone calls to the Service Desk during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.5 Call Abandonment Rate

Table 16 - Call Abandonment Rate

CALL ABANDONMENT RATE			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	N/A	≤ 5%
	Formula	[Number of phone calls to the Service Desk during that Measurement Interval that are abandoned from the queue before being answered by a Service Desk agent] divided by [total number of phone calls that entered the queue during the Measurement Interval] multiplied by 100% = “Percent (%) Abandoned”	

CALL ABANDONMENT RATE		
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.7.4.6 Email Response Time

Table 17 - Email Response Time

EMAIL RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	≤ 1 hour	≥ 95%
	Formula	[Number of e-mails received and responded to within the Target Performance during the Measurement Interval] divided by [total number of e-mails received during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.7 Voice Mail Response Time

Table 18 - Voice Mail Response Time

VOICE MAIL RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	≤ 30 minutes	≥ 95%
	Formula	[Number of voice mails received by the voicemail system during the Measurement Interval and responded to by a Service Desk agent within the Target Performance] divided by [total number of voice mails received by the voicemail system during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.8 Incident Acceptance Response Time

Table 19 - Incident Acceptance Response Time

INCIDENT ACCEPTANCE RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Severity 1 Incident: ≤15 elapsed minutes Severity 2 Incident: ≤ 15 elapsed minutes Severity 3 Incident: ≤ 2 Standard Operating Hours Severity 4 Incident: ≤ 4 Standard Operating Hours	≥ 95% (all Severity Levels)
	Formula	[Number of Incidents (of all Severity Levels) received and accepted (i.e., received, logged, and assigned) within the Target Performance during the Measurement Interval] divided by [total number of Incidents (of all Severity Levels) received and accepted during the Measurement Interval] multiplied by 100% = "Percent (%) Attained"	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.9 Service Request Acceptance Response Time

Table 20 - Service Request Acceptance Response Time

SERVICE REQUEST ACCEPTANCE RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Emergency Service Requests: ≤ 1 elapsed hour Other: ≤ 16 Standard Operating Hours	≥ 95% (both types)
	Formula	[Number of Service Requests (both types) received and accepted (received, logged, and assigned) within the Target Performance during the Measurement Interval] divided by [total number of Service Requests (both types) received and accepted during Measurement	

SERVICE REQUEST ACCEPTANCE RESPONSE TIME		
		Interval] multiplied by 100% = "Percent (%) Attained"
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.7.4.10 Incident Management: First Contact Resolution

Table 21 - Incident Management: First Contact Resolution

INCIDENT MANAGEMENT: FIRST CONTACT RESOLUTION			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	N/A	≥ 80%
	Formula	[Number of User contacts to the Service Desk during the Measurement Interval which are resolved by the initially-contacted Service Desk agent and did not result in a Call Back] divided by [the total number of User contacts during the Measurement Interval] multiplied by 100% = "Percent (%) Attained"	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.11 Incident Management: First Contact Call Back

Table 22 - Incident Management: First Contact Call Back

INCIDENT MANAGEMENT: FIRST CONTACT CALL BACK			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	N/A	< 5% Call Backs
	Formula	[Number of User contacts during the Measurement Interval which result in a Call Back] divided by [the total number of User contacts during the Measurement Interval] multiplied by 100% = "Percent (%) Call Backs"	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.12 Incident Management: Incident Resolution Time

Table 23 - Incident Management: Incident Resolution Time

INCIDENT MANAGEMENT: INCIDENT RESOLUTION TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Severity 1 Incident: ≤ 4 elapsed hours Severity 2 Incident: ≤ 6 elapsed hours Severity 3 Incident: ≤ 24 Standard Operating Hours Severity 4 Incident: ≤ 120 Standard Operating Hours	Severity 1 Incidents: ≥ 95% Severity 2 Incidents: ≥ 95% Severity 3 Incidents: ≥ 90% Severity 4 Incident: ≥ 90%
	Formula	[Number of Incidents received during the Measurement Interval which are Resolved within the Target Performance] divided by [total number of Incidents received during the Measurement Interval] multiplied by 100% = "Percent (%) Attained"	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.13 Incident Management: Incident and Service Request Closure Notice to Users

Table 24 - Incident Management: Incident and Service Request Closure Notice to Users

INCIDENT MANAGEMENT: INCIDENT AND SERVICE REQUEST CLOSURE NOTICE TO USERS			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	< 20 minutes of Resolution of Incident or Service Request completion	≥ 98%
	Formula	[Number of Incidents Resolved and Service Requests completed during the Measurement Interval for which a closure notice was provided to the User within the Target Performance] divided by [total number of Incidents Resolved and Service Requests completed	

INCIDENT MANAGEMENT: INCIDENT AND SERVICE REQUEST CLOSURE NOTICE TO USERS		
		during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.7.4.14 Incident Management: Incident and Service Request Resolution Rate

Table 25 - Incident Management: Incident and service request Resolution Rate

INCIDENT MANAGEMENT: INCIDENT AND SERVICE REQUEST RESOLUTION RATE			
Service Desk Availability	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Incidents: Severity 1 Incident: ≤ 24 elapsed hours Severity 2 Incident: ≤ 24 elapsed hours Severity 3 Incident: ≤ 120 elapsed hours Severity 4 Incident: ≤ 240 elapsed hours Service Requests: Emergency Service Requests: 24 elapsed hours Others: 120 elapsed hours	Incidents (all Severity Levels): 100% Service Requests (both types): 100%
	Formula	[Number of Incidents or Service Requests during the Measurement Interval which are Resolved or completed, as applicable, and closed within the Target Performance] divided by [total number of Incidents or Service Requests that are open (in the queue) during the Measurement Interval] multiplied by 100% = “Percent (%) Attained” This formula is applied separately to Incidents and Service Requests.	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.15 Incident Management: Incident Resolution Escalation to Level 2 Support

Table 26 - Incident Management: Incident Resolution Escalation to Level 2 Support

INCIDENT MANAGEMENT: INCIDENT RESOLUTION ESCALATION TO LEVEL 2 SUPPORT			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	When Contractor determines that an Incident requires Level 2 support, Contractor must escalate such Incident to Level 2 support within 15 minutes of such determination	≥ 95%
	Formula	[Number of Incidents requiring escalation to Level 2 support during the Measurement Interval that are forwarded to Level 2 support within the Target Performance] divided by [total number of Incidents requiring escalation to Level 2 support during the Measurement Interval] multiplied by 100% = "Percent (%) Attained"	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.7.4.16 Performance Management: Periodic User Satisfaction Sample Volume

Table 27 - Performance Management: Periodic User Satisfaction Sample Volume

PERFORMANCE MANAGEMENT: PERIODIC USER SATISFACTION SAMPLE VOLUME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	N/A	50% of Users who submitted a Service Request (with the exception of password reset Service Requests) or an Incident Request received a User satisfaction survey within 72 hours of Resolution or completion.
	Formula	[Number of Users submitting a qualifying Service Desk contact who receive a User satisfaction survey during the Measurement Interval] divided by [total number of Users submitting a qualifying Service Desk contact	

PERFORMANCE MANAGEMENT: PERIODIC USER SATISFACTION SAMPLE VOLUME		
		during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.7.4.17 Performance Management: User Satisfaction Service Level

Table 28 - Performance Management: User satisfaction Service Level

PERFORMANCE MANAGEMENT: USER SATISFACTION SERVICE LEVEL			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Users surveyed are “very satisfied” or “satisfied”.	≥ 80%
	Formula	[Number of User satisfaction survey responses received during the Measurement Interval with satisfaction ratings meeting the Target Performance] divided by [total number of User satisfaction survey responses received during the Measurement Interval] times 100% = “Percent (%) Attained”	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8 SERVICE MANAGEMENT

The Service Management section of the Statement of Work will be further reviewed with the Contractor upon Contract award. The RACI charts below depict an overall suggested approach that may change.

3.8.1 Service Objectives

The following are the key high-level service objectives the GC expects to achieve through EPS Service Management:

- to manage assets consistent with GC fiduciary obligations;
- to accurately, securely and consistently receive, value, transact and distribute participant funds with 100% reliability;
- to apply best-in-class internal business processes to ensure secure and efficient operations;
- to foster strong relationships with external GC partners to support legislative, regulatory and programmatic initiatives;

- to provide thorough and sound advice to enable GC leadership and management in making prudent decisions; To ensure that critical Information Technology (IT) lifecycle and Service Management functions and processes are included in IT SOWs;
- to ensure that all critical IT lifecycle and Service Management functions and processes are defined with clearly delineated roles and responsibilities, touch points and measurements between the GC and the Supplier;
- to receive IT Services that take into consideration an end-to-end enterprise and lifecycle view across all relevant IT Service Tiers; and
- to ensure all common activities across suppliers have consistent accountabilities between the GC and the supplier.

Another key objective of the EPS is to attain Service Level Requirements (SLR). SLRs applicable are identified in the Cross Functional SOW.

The ensuing SLRs contained in section 3.8.7 IT Service Levels represent the minimum Service levels required. The Contractor must meet or exceed the SLRs.

3.8.2 Structure

The scope of services described herein include the set of common services and processes that make up Service Management (sometimes also called "cross-functional, as well the services and processes required to support the IT service line SOWs. This refers to the broad categories of infrastructure, Application Services, Network Services (the domain of Shared Services Canada (SSC)), Service Desk Services, Transition Services, and end-user services.

3.8.3 Cross-functional Services

3.8.3.1 General Responsibilities

The following table identifies general roles and responsibilities associated with this SOW.

Table 29 - Service Management - General Roles and responsibilities

General Roles and Responsibilities	Contractor	GC
Provide Services and the supporting processes that support GC business needs, technical and End User requirements.	R	A
Approve Services and the supporting processes that support GC business needs, technical and End User requirements.	C	R
Comply with GC guiding principles, policies, standards and regulatory requirements applicable to GC for information, information systems, personnel, physical, and technical security.	R	A
Develop and maintain standards, processes and procedures that will be used in the delivery of all Services. The manual will include clearly delineated roles and responsibilities and measurements between GC and the Contractor.	R	A
Approve the comprehensive standards, processes and procedures that will be used in the delivery of services.	C	R

General Roles and Responsibilities	Contractor	GC
Conform to changes in laws, regulations and policies. Major Service Changes must be proposed on a project-by-project effort basis to alter the environment to conform to the new requirements.	R	A
Report performance against Service Level Requirements ("SLRs").	R	A
Coordinate all Changes to the IT infrastructure.	R	A
Provide timely creation, updating, maintenance and provisioning of all appropriate plans, time and cost estimates, technical specifications, management documentation and management reporting in a format that is acceptable to GC for all major Service Changes.	R	A
Adhere to ITIL best practices and GC approved Key Performance Indicators (KPI).	R	A
Approve the use of the ITIL best practices and Key Performance Indicators.	C	R

3.8.4 IT Life Cycle and Operations

3.8.4.1 Planning and Analysis

Planning and Analysis Services are activities associated with researching new technical trends, products and services, such as hardware components, system software and networks that offer opportunities to improve the efficiency and effectiveness. Planning and Analysis Services can also help support competitive business advantage and mitigate risks by reducing defects and improving the quality of IT Services. The following table identifies the Planning and Analysis roles and responsibilities, respectively of the Contractor and GC.

Table 30 - IT Life Cycle and Operations - Planning and Analysis

Planning and Analysis Roles and Responsibilities	Contractor	GC
Provide corporate business goals and objectives, information system roadmaps, IT governance model and, IT risk issues and opportunities.	I	R
Define Services, processes, and standards for Planning and Analysis Services.	R	A
Review and approve Services, processes, and standards for Planning and Analysis Services.	C	R
Define GC requirements at the enterprise level (e.g., business, technology strategy, functional, availability, capacity, performance, backup and IT service continuity).	C	R
Perform Service Planning and Analysis based on GC requirements (e.g., availability, capacity, performance, and Disaster Recovery Services).	R	A
Provide recommendations for new or changes to; in scope applications, infrastructure, processes, and Services based on Planning and Analysis Service results.	R	A
Approve recommendations for new or changes to: applications, infrastructure, processes and Services.	C	R
Provide management reports required for Planning and Analysis Services (e.g., utilization and capacity trend reports, rollout plans).	R	A
Define Data Backup and Retention policies.	C	R

Planning and Analysis Roles and Responsibilities	Contractor	GC
Continuously monitor technical trends through independent research; document and report on products, processes and services with potential use to align with GC business and technology strategy.	R	A
Perform feasibility studies for the implementation of new technologies that best meet GC business needs and meet cost, performance and quality objectives.	R	A
Define enterprise-level deployment management policies, procedures and requirements (e.g., feasibility analysis, cost-benefit analysis, scheduling, costing, resource planning, communication planning, procurement, risk management and quality management).	C	R
Perform management function for Contractor-managed activities.	R	A
Perform management oversight and liaison function to the business.	I	R
Conduct regular planning for technology refreshes and upgrades.	R	A
Participate in regular planning for technology refreshes and upgrades.	C	R
Conduct quarterly technical reviews and provide recommendations for IT Service improvements that align to GC business goals.	R	A

3.8.4.2 Requirements Definition

Requirements Definition Services are the activities associated with the assessment and definition of functional, performance, IT Continuity and Disaster Recovery, and Security requirements. These requirements drive the technical design for the environment. The following table identifies the Requirements Definition roles and responsibilities, respectively of the Contractor and GC.

Table 31 - IT Life Cycle and Operations - Requirements Definitions

Requirements Definition Roles and Responsibilities	Contractor	GC
Define and document requirements for the technical design of the environment.	C	R
Participate in defining requirements for the technical design of the environment.	R	A
Document requirements to deliver Services in a GC agreed to formats.	R	A
Ensure requirements meet GC policies, procedures and applicable government regulations.	R	A
Approve all requirements.	I	R
Define Acceptance Test Criteria.	R	A
Review and approve all Acceptance Test Criteria.	I	R
Provide documented requirements and Acceptance Test Criteria per approved requirements standards.	R	A

3.8.4.3 Design Specifications

Design Specification services are the activities and deliverables associated with translating user and information system requirements into detailed technical specifications. The following table identifies the Design Specification roles and responsibilities, respectively of the Contractor and GC.

Table 32 - IT Life Cycle and Operations - Design Specifications

Design Specifications Roles and Responsibilities	Contractor	GC
Define Design Specifications Services standards and requirements.	C	R
Develop, document and maintain technical design plans and environment configuration based on GC Design Specifications Services standards and requirements including IT architecture, functional, performance, Availability, maintainability, security and Disaster Recovery requirements.	R	A
Determine and document required component upgrade, replacement and/or conversion specifications (e.g., Equipment, Software, Networks).	R	A
Review and approve design plans through coordination with the appropriate GC technology standards group and design architects.	I	R
Conduct site surveys for design efforts as required.	R	A
Provide written information in sufficient detail pertaining to the Design Specifications to enable creation of the appropriate design documents.	C	R
Document and deliver Design Specifications.	R	A
Review and approve Design Specifications.	I	R

3.8.4.4 Technology Architecture

Technology Architecture are the activities associated with the design and development of the IT infrastructure and tools that support the IT Service. The following table identifies the Service-Level Monitoring and Reporting roles and responsibilities, respectively of the Contractor and GC.

Table 33 - IT Life Cycle and operations - Technology Architecture

Technology Architecture Roles and Responsibilities	Contractor	GC
Recommend Technology Architecture Services for the design and development of the IT infrastructure and tools required to support the IT Service.	R	A
Review and approve Technology Architecture Services design and development requirements.	I	R
Develop and document Technology Architecture Service designs and plans that meet requirements and adhere to defined policies.	R	A
Review and approve Technology Architecture Service designs and plans.	I	R
Implement design for changes to existing or new IT Services.	R	A

3.8.4.5 Service-Level Monitoring and Reporting

Service-Level Monitoring and Reporting Services are the activities associated with the monitoring and reporting Service Levels with respect to Service-Level Requirements (SLRs). The following table identifies the Service-Level Monitoring and Reporting roles and responsibilities, respectively of the Contractor and GC.

Table 34 - Service-Level Monitoring and Reporting Responsibilities

Service-Level Monitoring Roles and Responsibilities	Contractor	GC
Define Service-Level requirements	I	R
Define Service-Level Monitoring and Reporting requirements and policies	I	R

Service-Level Monitoring Roles and Responsibilities	Contractor	GC
Develop, document and maintain in the Standards Process and Procedures Manual Service-Level Monitoring and Reporting procedures that meet requirements and adhere to defined policies	R	A
Review and approve Service-Level Monitoring and Reporting procedures	I	R
Report on SLR performance and improvement results	R	A
Coordinate SLR monitoring and reporting with designated Client representative and Third Parties	R	A
Measure, analyze and provide management reports on performance relative to SLRs	R	A
Conduct SLR Improvement Meetings to review SLRs and recommendations for improvements	R	A
Review and approve SLR improvement plans	I	R
Implement SLR improvement plans	R	A
Review and approve SLR metrics and performance reports	I	R
Provide GC with access to performance and SLR reporting and monitoring system and data	R	A

3.8.4.6 Performance Management

Performance Management Services are the activities associated with managing and tuning Service components for optimal performance. The following table identifies the Performance Management roles and responsibilities, respectively of the Contractor and GC.

Table 35 - Performance Management Roles and Responsibilities

Performance Management Roles and Responsibilities	Contractor	GC
Define Performance Management requirements and policies	I	R
Develop, document and maintain in the Standards, Process and Procedures Manual Performance Management procedures that meet requirements and adhere to defined policies	R	A
Review and approve Performance Management procedures	I	R
Perform Service component tuning to maintain optimum performance in accordance with Change Management procedures	R	A
Manage Service component resources (e.g., devices and traffic) to meet defined Availability and performance SLRs	R	A
Provide monitoring and reporting of Service component performance, utilization and efficiency based on specified time frame and sequence (e.g., monthly)	R	A
Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance	R	A
Conduct trending analysis to recommend changes to improve the performance based on specified time frame and sequence (e.g., monthly)	R	A
Develop and deliver improvement plans as required to meet SLRs based on specified time frame and sequence (e.g., monthly)	R	A
Review and approve improvement plans	R	R
Implement improvement plans and coordinate with Third Parties as required	R	A

Performance Management Roles and Responsibilities	Contractor	GC
Provide technical advice and support to the application maintenance and development staffs as required	R	A

3.8.4.7 Availability Management

Availability Management is the overall availability requirements of GC business needs and to plan, measure, monitor and continuously strive to improve the availability of the IT Infrastructure, services and supporting IT organization. Availability Management covers the evaluation, design, implementation, measurement and management of the IT Infrastructure Availability from a component and an end-to-end perspective.

The following table identifies the Availability Management roles and responsibilities, respectively of the Contractor and GC.

Table 36 - IT Life cycle and Operations - Service Delivery: Availability Management

Availability Management Roles and Responsibilities	Contractor	GC
Establish criteria and SLRs for Availability Management support requirements, including IT systems and services to be covered.	C	R
Develop Availability Management policies, process and procedures and determine appropriate Availability Management tools and methods that support GC's Availability Management support requirements.	R	A
Participate in the development of Availability Management policies, process and procedures and identifying the tools and availability methods to be used.	C	R
Review and approve Availability Management policies, processes and procedures.	I	R
Implement agreed-upon Availability Management policies, processes and procedures.	R	A
Provide unrestricted read access by GC-authorized staff and designated personnel to all Availability knowledgebase data and records from the applicable Commencement date.	R	A
Provide unrestricted read access to GC-authorized Contractor staff and designated personnel to all historical Availability knowledgebase data and records prior to the applicable Commencement date.	I	R
Ensure that Availability requirements are included when requirements are identified when upgrading and/or designing new IT systems and services to support business users.	I	R
Participate in user requirements gathering and analysis when upgrading and/or designing new IT systems and services to ensure that IT Services and systems are designed to deliver the required levels of Availability (mapped to the SLRs) required by the business.	R	A
Create Availability and recovery design criteria to be applied to upgrades and/or new or enhanced Infrastructure design.	R	A
Participate in creating Availability and recovery design criteria to be applied to upgrades and/or new IT Infrastructure system and services design.	C	R

Availability Management Roles and Responsibilities	Contractor	GC
Coordinate with the IT service support and IT service delivery process owners and managers from GC to research, review, and assess Availability issues and optimization opportunities.	R	A
Define the Availability measures and reporting required for the IT Infrastructure and its components.	I	R
Participate with GC in defining the Availability measures and reporting requirements.	R	A
Recommend appropriate tools and practices to measure and report on agreed-upon Availability measures for upgraded and/or enhanced IT Infrastructure.	R	A
Review and approve Availability measurement tools and practices.	I	R
Ensure that approved Availability measurement tools and practices are implemented.	R	A
Monitor and maintain an awareness of technology advancements and IT best practices related to Availability optimization and periodically provide updates to GC IT management.	R	A
Ensure that all Availability Management improvement initiatives conform to defined Change Management procedures set forth in the Standards and Operations Procedures.	R	A
Work with GC and third-parties (e.g., public carriers, Internet service Suppliers, third party vendors, etc.) to meet Availability SLRs and otherwise fulfill the requirements of the Availability Management section of this SOW.	R	A
Lead Problem Management review sessions as appropriate, specifically those Problems related to outages of critical systems.	R	A
Monitor actual IT Availability achieved versus targets and ensure shortfalls are addressed promptly and effectively.	R	A
Conduct Availability Assessment review sessions and provide improvement recommendations.	R	A
Participate in Availability review sessions.	C	R
Review and approve improvement recommendations.	I	R
Coordinate with GC and third-party service Suppliers to gather information on IT systems and service Availability issues and trends to be used for trend analysis.	R	A
Produce and maintain an Availability Plan which prioritizes and plans approved IT Availability improvements.	R	A
Review and approve Availability Plan.	I	R
Provide IT Availability reporting to ensure that agreed levels of Availability, reliability, and maintainability are measured, reported and monitored on an ongoing basis.	R	A
Promote Availability Management awareness and understanding within all IT support organization including third party service Suppliers.	R	A
Perform regular reviews of the Availability Management process and its associated techniques and methods to ensure that all are subjected to continuous improvement and remain fit for purpose.	R	A
Periodically audit the Availability Management process to ensure that it continues to deliver desired results in compliance with agreed-upon policies, processes and procedures.	I	R

3.8.4.8 Capacity Management

Capacity Management Services are the activities associated with ensuring that the capacity of the Services matches the evolving demands of Client business in the most cost-effective and timely manner. The following table identifies the Capacity Management roles and responsibilities, respectively of the Contractor and GC.

Table 37 - IT Life Cycle and Operations - Service delivery: Capacity Management

Capacity Management Roles and Responsibilities	Contractor	GC
Define Capacity Management requirements (SLRs) and policies.	I	R
Develop, document and maintain Capacity Management procedures that meet requirements and adhere to defined policies.	R	A
Review and approve Capacity Management process and procedures.	I	R
Establish a comprehensive Capacity Management planning process.	R	A
Review and approve Capacity Management planning process.	I	R
Define, develop and implement tools that allow for the effective capacity monitoring/trending of IT infrastructure, applications and IT components.	R	A
Identify future business requirements that will alter capacity requirements.	I	R
Develop a quarterly capacity plan.	R	A
Develop and implement capacity models to validate the capacity plan.	R	A
Participate in capacity planning activities where applicable.	C	R
Assess capacity impacts when adding, removing or modifying applications and infrastructure components.	R	A
Continually monitor IT resource usage to enable proactive identification of capacity and performance issues.	R	A
Capture trending information and forecast future GC capacity requirements based on GC-defined thresholds.	R	A
Assess Incidents/Problems related to capacity and provide recommendations for resolution.	R	A
Recommend changes to capacity to improve service performance.	R	A
Assess impact/risk and cost of capacity changes.	R	A
Approve capacity-related recommendations.	I	R
Maintain capacity levels to optimize use of existing IT resources and minimize GC costs to deliver Services at agreed-to SLRs.	R	A
Ensure adequate capacity exists within the IT environment to meet SLR requirements taking into account daily, weekly and seasonal variations in capacity demands.	R	A
Validate Asset utilization and capital efficiency.	C	R

3.8.4.9 Backup and Recovery

Backup and Recovery Services are the activities associated with providing ongoing Backup and Recovery capabilities according to GC schedules and requirements. The Contractor must demonstrate that it will consistently meet or exceed GC's ongoing Backup and Recovery requirements. The following table identifies Backup and Recovery roles and responsibilities, respectively of the Contractor and GC.

Table 38 - IT Life Cycle and operations - Service Delivery: Backup and Recovery

Backup and Recovery Roles and Responsibilities	Contractor	GC
Define Backup and Recovery schedules, requirements and policies.	I	R
Recommend best practices for Backup and Recovery Services strategies, policies, and process and procedures.	R	A
Develop, document and maintain Backup and Recovery schedules and procedures that adhere to GC requirements and policies.	R	A
Coordinate the Backup and Recovery Standards with GC Security and Legal teams.	R	A
Review and approve Backup and Recovery schedules and process and procedures.	I	R
Define Backup and Recovery Monitoring and Reporting requirements and policies.	I	R
Manage backup media inventory (tape, disk, optical and other media type) including the ordering and distribution of media.	R	A
Perform Service component backups and associated rotation of media as required.	R	A
Identify and establish a secure off-site location for data media.	I	R
Approve secure off-site location for data media.	I	R
Archive data media at a secure off-site location.	I	R
Ensure ongoing capability to recover archived data from media as specified (backward compatibility of newer backup equipment or maintaining equipment in operation as of the Effective Date) by using GC provided Hardware and Software, or providing new capability through a proposed Project. The Contractor must ensure that data that is written on Contractor provided equipment will be readable throughout the term of the Contract.	R	A
Test backup media to ensure incremental and full recovery of data is possible and ensure Service component integrity, as required or requested by GC.	R	A
Recover files, file system or other data required from backup media, as required or requested by GC.	R	A
Provide recovery and backup requirements and updates as they change.	I	R
Provide GC access to backup and recovery reporting and monitoring systems and data.	R	A

3.8.4.10 IT Service Continuity and Disaster Recovery (DR)

IT Service Continuity and Disaster Recovery (DR) Services are the activities associated with providing such Services for GC applications, and their associated infrastructure (e.g., CPU, servers, network, data and output devices, End-User devices) and for Voice Network Services. GC applications, associated infrastructure and Voice Network Services will receive DR Services according to GC's Business Continuity Plan. The Contractor must demonstrate that it will consistently meet or exceed GC's IT Service Continuity and DR Services requirements. The following table identifies Service Continuity and DR Services roles and responsibilities, respectively of the Contractor and GC.

Table 39 - IT Life Cycle and operations - Service Delivery: Service Continuity & Disaster Recovery

Service Continuity & Disaster Recovery Roles and Responsibilities	Contractor	GC
Define Disaster Recovery Services strategy, requirements and policies.	I	R
Recommend best practices for Disaster Recovery Services strategies, policies, process and procedures.	R	A
Document Disaster Recovery Services process and procedures that adhere to GC requirements and policies.	R	A
Review and approve Disaster Recovery Services procedures.	I	R
As needed, assist GC in other IT continuity and emergency management activities.	R	A
Develop and maintain a detailed DR plan to meet Disaster Recovery requirements. Plan must include plans for data, backups, storage management and contingency operations that provide for recovering GC's systems within established recovery requirement time frames after a disaster affects GC's use of the Services.	R	A
Define data (file system, database, flat files, etc.) replication, backup and retention requirements.	I	R
Establish processes to ensure DR plans are kept up to date and reflect Changes in GC environment.	R	A
Establish procedures to ensure the impact to the DR plans are reviewed by the Change Management process.	R	A
Review and approve DR plans.	I	R
Establish DR test requirements.	C	R
Perform scheduled DR tests per GC policies.	R	A
Coordinate involvement of users for DR testing.	I	R
Participate in DR tests.	C	R
Track and report DR test results to GC.	R	A
Review and approve DR testing results.	I	R
Develop action plan to address DR testing results.	R	A
Review and approve DR testing action plan.	I	R
Implement action plan and provide ongoing status until completion.	R	A
Initiate the DR plan in the event of a GC DR situation per the DR policies and procedures.	I	R
Initiate the DR plan in the event of a Contractor DR situation and notify GC per DR policies and procedures.	R	A
Coordinate with GC during a Contractor DR situation per DR policies and procedures.	R	A
Provide GC Disaster Recovery Reports.	R	A

3.8.4.11 Service Delivery: Financial/Chargeback Management

Financial/Chargeback Management and Visibility are the activities associated with providing data that allows GC to charge back its internal business. The following table identifies Security roles and responsibilities, respectively of the Contractor and GC.

Table 40 - IT Life Cycle and operations - Service delivery: Financial/Chargeback Management

Financial/Chargeback Management and Invoicing Roles and Responsibilities	Contractor	GC
Identify the Chargeback components and map to the business services.	I	R
Define Financial/Chargeback and Invoicing Management requirements and policies.	I	R
Assist GC in documenting Financial/Chargeback and Invoicing processes.	R	A
Review and approve Financial/Chargeback and Invoicing Management processes.	I	R
Provide Chargeback reports and data at level of detail and in a format as defined in GC requirements.	R	A
Review and approve Chargeback reports.	I	R
Conduct review meetings.	R	A

3.8.4.12 Security

Security Services are the activities associated with maintaining physical and logical security of all IT Service components (hardware and software) and data, virus protection, access protection and other Security Services in compliance with GC Security requirements and NIST. The following table identifies Security roles and responsibilities, respectively of the Contractor and GC. Security requirements are fully elaborated in Annex 2-Security and Privacy Requirements.

Table 41 - IT Life Cycle and Operations – Service Delivery: Security

Security Roles and Responsibilities	Contractor	GC
Define Security requirements, standards, process and procedures and policies including regulatory requirements.	I	R
Assist in developing Security standards, policies and procedures including industry best practices.	R	A
Develop, document and maintain requirements standards, process and procedures and policies including regulatory requirements.	R	A
Review and approve Security requirements, standards, procedures and policies including regulatory requirements.	I	R
Remain up to date with current Security trends, threats, common exploits and security policies and procedures and best practices.	R	A
Provide an Information Security Advisor that will be the direct liaison with GC for Security requirements.	R	A
Conduct risk assessments to identify control or Security gaps.	C	R
Provide Security plan and IT infrastructure based on Security requirements, standards, procedures, policies, federal, state, and local requirements and risks.	R	A
Review and approve Security plans.	I	R
Implement physical and logical Security plans consistent with GC Security policies and industry standards in Contractor facilities (e.g., ISO 27001, COBIT).	R	A
Establish access profiles and policies for adding, changing, enabling/disabling and deleting log-on access of GC employees, agents and subcontractors.	I	R

Security Roles and Responsibilities	Contractor	GC
Perform Security-level access changes as detailed in profiles and policies for all Services Towers.	R	A
Provide and support best in-class Software as a Service (SaaS) Security analysis and monitoring products into GC's system and Network infrastructure.	R	A
Report and Resolve Security Incidents to GC per GC policies.	R	A
Review all Security patches relevant to the IT environment and classify the need and speed in which the Security patches should be installed as defined by Security policies and Change Management.	R	A
Install Security patches per GC's Change Management process and procedures.	R	A
Assist GC to develop a security awareness program by providing expert advice based on best practices in the industry.	R	A
Implement a sustained security awareness program.	R	A
Maintain all documentation required for Security assessments, audits and internal control and control testing.	R	A
Perform periodic Security audits.	I	R
Allow Third Party Security audits.	R	A
Provide GC access to Contractor security reporting and monitoring systems and data.	R	A

3.8.4.13 Security Operations Centre

The Contractor must provide a Security Operations Centre (SOC), prior to the commencement of Steady State operations, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, and 365 days per year) of GC EPS Security Incidents.

The Security Operations Center (SOC) must:

- coordinate Security Incident response in close coordination with GC;
- include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller;
- act as a point of contact for communications with GC representatives for security incidents;
- not impact operations of GC EPS Services in case of a Contractor SOC failure; and
- notify GC within 15 minutes if Contractor SOC is not available and provide a contact name that GC can communicate as necessary during the Contractor SOC outage.

The SOC must work with PWGSCs Information Protection Centre for activities that include: integration of processes; oversight; Security Incident handling and response; and auditing.

The SOC must accept emails from GC authorized users to a Contractor-provided mailbox with an auto reply to confirm receipt of the email. The SOC personnel must acknowledge receipt of emails received within 15 minutes of receiving the email 24 hours per day, 7 days per week, and 365 days per year. The SOC must authenticate the identity of the requester using a process approved by GC.

3.8.5 Service Operations and Support

3.8.5.1 Change Management

Change Management Services are activities to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change upon Service quality and consequently to improve the day-to-day operations of GC.

The Change Management processes and activities are inter-related and complementary with Release Management and Configuration Management, as well as Incident Management and Problem Management.

The following table identifies Change Management roles and responsibilities, respectively of the Contractor and GC.

Table 42 - IT Life Cycle and Operations – Service Support: Change Management

Change Management Roles and Responsibilities	Contractor	GC
Recommend Change Management policies, procedures, processes and training requirements per the Change Management process components outlined above, including Change Advisory Board (CAB) composition, activities, and the financial, technical, and business approval authorities appropriate to GC IT and business requirements.	R	A
Participate in the development of the Change Management and CAB procedures, policies, and approval authorities.	C	R
Establish change priority schema and classifications (impact, priority, risk) and change authorization process.	R	A
Review and Approve Change Management process, procedures and policies.	I	R
Receive and document all Requests for Change (RFC) and classify proposed changes to the Services, which must include change cost, risk impact assessment, and system(s) security considerations.	R	A
Review and approve non-preapproved RFCs.	I	R
Ensure that appropriate back-out plans are documented and in place in the event of systems failure as a result of the change.	R	A
Provide Change Management plan to GC for review.	R	A
Approve Change Management plan.	I	R
Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes or FSC) for GC to review.	R	A
Identify change logistics.	R	A
Provide change documentation as required, including proposed metrics as to how effectiveness of the change will be measured.	R	A
Review and approve change documentation and change effectiveness metrics.	I	R
Coordinate, schedule, and conduct Change Advisory Board (CAB) meetings to include review of planned changes and results of changes made, ensuring that all appropriate parties are invited and represented in accordance with approved CAB policies.	R	A
Participate in CAB meetings as GC deems appropriate or necessary.	C	R

Change Management Roles and Responsibilities	Contractor	GC
Authorize and approve scheduled changes or alter the schedule change requests as defined in the Change Management procedures.	I	R
Publish and communicate the approved FSC (Forward Schedule of Changes) to all appropriate IT and business unit stakeholders within GC of change timing and impact.	R	A
Oversee the approved change build, test, and implementation processes to ensure these activities are appropriately resourced and completed according to Change schedule.	R	A
Ensure that thorough testing is performed prior to release and assess GC business risk related to any change that is not fully tested prior to implementation.	R	A
Participate in business risk assessment for change to be introduced without being fully tested.	C	R
Monitor changes, perform change reviews and report results of changes, impacts, and change effectiveness metrics.	R	A
Verify that change met objectives based upon predetermined effectiveness metrics and determine follow-up actions to resolve situations where the change failed to meet objects.	R	A
Review and approve change management results.	I	R
Close out RFCs that met the change objectives or changes that were abandoned.	R	A
Perform Change Management quality control reviews.	R	A
Perform audits of Change Management processes and records.	I	R
Provide GC Change Management reports as required and defined by GC.	R	A

3.8.5.2 Configuration Management

Configuration Management Services are the activities associated with providing a logical model of the IT Services devices or assets (including software licenses) and their relationships by identifying, controlling, maintaining and verifying installed hardware, software and documentation (i.e., maintenance contracts, SLA documents, etc.).

The following table identifies the Configuration Management roles and responsibilities, respectively of the Contractor and GC.

Table 43 - IT Life Cycle and Operations – Service Support: Configuration Management

Configuration Management Roles and Responsibilities	Contractor	GC
Define Configuration Management requirements and policies.	R	A
Develop, document and maintain Configuration Management procedures that meet requirements and adhere to defined policies.	R	A
Review and approve Configuration Management procedures and processes.	I	R
Identify and document the Configuration Item structure.	R	A
Approve the Configuration Item structure.	I	R
Establish Configuration Management Database (CMDB), in accordance with GC requirements.	R	A
Review and approve CMDB.	I	R

Configuration Management Roles and Responsibilities	Contractor	GC
Select, install and maintain Configuration Management tools.	R	A
Review and approve Configuration Management tools.	I	R
Enter/upload configuration data into configuration database.	R	A
Establish process and data interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes and tools.	R	A
Establish appropriate authorization controls for modifying configuration items and verify compliance with Software licensing.	R	A
Proactively update and incorporate deficiencies into CMDB and interfaced tools and processes.	R	A
Establish guidelines for physical and logical separation between path to production and production and the process for deploying and back-out of configuration items.	R	A
Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states.	R	A
Establish procedures for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies.	R	A
Provide a Configuration Management deficiency report and steps taken to address the issues identified.	R	A
Provide GC Configuration Management reports as required and defined by GC.	R	A
Audit Configuration Management process and accuracy of configuration data.	I	R

3.8.5.3 Release Management

Release Management Services are activities related to implementing changes to define IT services and covers both the software and the hardware. Release Management Services take a holistic view of a change to a Service to ensure that the technical and non-technical aspects of a release related to software and hardware changes.

These changes can be implemented by rolling out a combination of new applications or infrastructure software and/or upgraded or new hardware, or simply by making changes to the documentation, such as service hours or support arrangements. Release Management processes and activities are inter-related and complementary with the Change Management process, as well as Configuration Management and Problem Management.

The following table identifies Release Management roles and responsibilities, respectively of the Contractor and GC.

Table 44 - IT Life Cycle and Operations – Service Support: Release Management

Release Management Roles and Responsibilities	Contractor	GC
Recommend Release Management policies, procedures, processes, and training requirements per the Release Management process components outlined above.	R	A

Release Management Roles and Responsibilities	Contractor	GC
Participate in the development of the Release Management process and procedures and policies.	C	R
Review and approve Release Management process procedures and policies.	I	R
Maintain an appropriate secure environment(s) where all authorized versions of all Software, in physical or electronic form as applicable (Definitive Software Library or DSL) and where all Equipment spares (Definitive Hardware Store or DHS) are stored, protected and accounted.	R	A
Maintain an appropriate secure environment(s) where all Equipment spares (Definitive Hardware Store or DHS) are stored, protected and accounted.	R	A
Ensure that all Equipment spares are secured in the DHS and reflected in the configuration management database(s).	R	A
Establish, manage, update, and maintain the overall Release Management Plan and Release Schedule for all planned Releases.	R	A
Establish and administer the version control schema as it relates to Release Management of GC custom applications.	R	A
Develop, manage, update and maintain formal Release Management Plans for each Release in coordination with Change Management.	R	A
Develop quality plans and back-out plans as appropriate for each Release.	R	A
Provide Release Management Plans and Release Schedules to GC for review.	R	A
Review and approve Release Management Plans and Release Schedules.	I	R
Conduct site surveys, as necessary, to assess existing Equipment and Software being used to validate Release package requirements and dependencies.	R	A
Plan resource levels and requirements for supporting a Release.	R	A
Ensure that any new Software, Equipment, or support services required for the Release are procured and available when needed.	R	A
Ensure that all necessary testing environments are available and properly configured to support Release testing.	R	A
Ensure there is segregation of duties between the Application developer testers and the Release Management testers.	R	A
Conduct User Acceptance Testing (UAT) as required.	C	R
Schedule and conduct Release Management meetings to include review of planned releases and results of changes made.	R	A
Identify and document all Configurable Items (CIs) that need to be included in the Release, as well as all system inter-dependencies.	R	A
Plan and manage the acceptance testing process for each Release.	R	A
Review and approve Release acceptance testing plans.	I	R
Provide Release documentation as required.	R	A
Authorize and approve scheduled Releases or alter the schedule as defined in the Release Management procedures.	I	R
Review Release Management details and alter as appropriate to meet the needs of the GC (e.g., back out plan, go/no go decision).	R	A
Prepare user communication.	R	A
Review and approve communication.	I	R
Notify GC affected clients of Release timing and impact and provide communications to the service desk.	R	A

Release Management Roles and Responsibilities	Contractor	GC
Implement Release in compliance with Change Management requirements and adherence to detailed release plans.	R	A
Modify configuration database, asset management items, and service catalog (if applicable) to reflect changes to CIs due to the Release.	R	A
Conduct post-mortem of Releases that necessitated implementation of the backout plan and develop and implement appropriate corrective or follow-up actions to minimize future occurrences.	R	A
Perform quality control audits and approve Release control results.	I	R
Provide GC Release Management reports as required and defined by GC.	R	A

3.8.5.4 Identity and Access Management

Identity and Access Management (IAM) is a broad administrative area that establishes a unique identity for individuals and associates their established identity with user rights and privileges. It is an enterprise business strategy that governs the definition, storage, use and management of identities. The solution integrates business processes and technologies to authenticate, authorize provision and de-provision user access rights for resources across the enterprise. The following table identifies the Identity and Access Management roles and responsibilities, respectively of the Contractor and GC.

Table 45 - IT Life Cycle and Operations – Service Support: Identity and Access Management

Identity and Access Management Roles and Responsibilities	Contractor	GC
Support provisioning/de-provisioning of accounts for GC End User, service and system accounts as per GC policies and procedures.	R	A
Support provisioning/de-provisioning as currently defined.	R	A
Provide account re-validation (for example annual account attestation) and/or job role change process according to defined standards.	R	A
Maintain workflow processes to support multiple approvers, as currently defined by GC system with email notification used as a part of the workflow process.	R	A
Provide reporting on all access assigned to End Users, service and system accounts.	R	A
Provide ability to de-provision all access as defined in the Operations and Procedures Manual (automatically via integration with GC systems or manually).	R	A
Provide reporting capabilities to support audit and compliance requirements (ability to audit the requests and approvals).	R	A
Enable requestor to track their requests and/or approvals.	R	A
Support delegation of approvals.	R	A
Provide self-service account requests via Web interface.	R	A
Provide Self-service password reset capability via Web interface.	R	A
Synchronize password resets with all provisioned end points.	R	A
Provide Application and server infrastructure support and maintenance for GC IAM system.	R	A
Support SSO connections including application and server infrastructure support and maintenance.	R	A
Support Privileged Identity Management implementation, including application and server infrastructure support and maintenance.	R	A

3.8.5.5 Integration and Testing

Integration Services are the activities associated with ensuring the interoperability of the IT infrastructure within and across IT services and that all individual IT components configured with or added to the IT environment work together cohesively to achieve the intended results. The following table identifies the Integration roles and responsibilities, respectively of the Contractor and GC.

Table 46 - IT Life Cycle and Operations – Integration and Testing

Integration and Testing Roles and Responsibilities	Contractor	GC
Define Integration and Testing requirements and policies.	C	R
Develop, document and maintain Integration and Testing procedures and plans that meet requirements and adhere to defined policies.	R	A
Review and approve Integration and Testing procedures and plans.	I	R
Deploy and manage Integration and Testing environments.	R	A
Maintain Software Release Matrices across Integration and Testing environments.	R	A
Review and approve the Software Release Matrix.	I	R
Stage new and upgraded Service components or Services to Integration and Testing environment.	R	A
Assess and communicate the overall impact and potential risk to Service components prior to implementing Changes.	R	A
Conduct testing for all new and upgraded Service components or Services to include unit, system, integration, regression and user acceptance testing based on documented requirements and policies.	R	A
Validate all new and upgraded Service components or Services for compliance with GC security policies.	R	A
Perform modifications and adjustments to new and upgraded Service components or Services as a result of testing and validate results.	R	A
Review and approve new and upgraded Service components or Services test results.	I	R
Perform Configuration Management and Change Management activities related to Integration and Testing Services.	R	A
Ensure path to production environments maintain consistent configuration across all Service components.	R	A

3.8.5.6 Implementation and Migration

Implementation and Migration Services are the activities associated with the installation of new and upgraded IT components (e.g., hardware, software [operating system] and network components). The following table identifies the Implementation and Migration roles and responsibilities, respectively of the Contractor and GC.

Table 47 - IT Life Cycle and Operations – Implementation and Migration

Implementation and Migration Roles and Responsibilities	Contractor	GC
Define Implementation and Migration requirements and policies.	C	R
Develop, document and maintain Implementation and Migration procedures that meet requirements and adhere to defined policies.	R	A

Implementation and Migration Roles and Responsibilities	Contractor	GC
Review and approve Implementation and Migration Service procedures.	I	R
Notify GC of equipment migration and redeployment plans and schedules.	R	A
Review all Implementation and Migration plans and schedules with GC.	R	A
Approve Implementation and Migration plans and schedules.	I	R
Provide GC IT technical staff and End Users with training related to the Implementation and Migration to new and upgraded Service components or Services.	R	A
Conduct pre-installation site surveys, as required.	R	A
Coordinate physical infrastructure changes as required (e.g., wiring, cable plant, cooling, etc.).	R	A
Install physical infrastructure as required (e.g., wiring, cable plant, cooling, etc.) in GC managed facilities.	I	R
Coordinate Implementation and Migration support activities with GC IT staff and Contractor IT staff.	R	A
Install or migrate new and upgraded Service components or Services into operational environment.	R	A
Perform validation tests on all new and upgraded Service components or Services.	R	A
Approve successful implementation of new and upgraded Service components or Services.	I	R
Update all documentation to new and upgraded Service components or Services.	R	A

3.8.5.7 Training and Knowledge Transfer

Training and Knowledge Transfer Services consist of the following three types of training the Contractor must provide:

- Training for the improvement of skills through education and instruction for Contractor's staff. The Contractor must participate in any initial and ongoing training delivered by GC as required that would provide a learning opportunity about GC's business and technical environment.
- Training for GC-retained technical staff for the express purpose of exploiting the functions and features of the GC computing environment. Delivery methods may include classroom-style, computer-based, individual or other appropriate means of instruction.
- Selected classroom-style and computer-based training (case-by-case basis) for standard Software as a Service (SaaS) applications, including new employee training, upgrade classes and specific skills.

The following table identifies the Training and Knowledge Transfer roles and responsibilities, respectively of the Contractor and GC.

Table 48 - IT Life Cycle and Operations – Training and Knowledge Transfer

Training and Knowledge Transfer Roles and Responsibilities	Contractor	GC
Define Training and Knowledge Transfer requirements and policies.	R	A
Develop, document and maintain Training and Knowledge Transfer procedures that meet requirements and adhere to defined policies.	R	A
Review and approve Training and Knowledge Transfer procedures.	I	R
Review and approve Contractor-developed training program.	I	R
Develop and deliver training program to instruct GC personnel on the provision of Contractor Services (e.g., "rules of engagement," requesting Services).	R	A
Develop, implement and maintain a GC-accessible knowledge database/portal.	R	A
Develop and implement Knowledge Transfer procedures to ensure that more than one individual understands key components of the business and technical environment.	R	A
Participate in GC-delivered instruction on the business and technical environment.	R	A
Develop, document and deliver training requirements that support the ongoing provision of GC Services, including refresher courses as needed and instruction on new functionality.	R	A
Take training classes as needed to remain current with systems, Software, features and functions for which Service Desk support is provided, in order to improve Service performance (e.g., First-Contact Resolution).	R	A
Provide training when substantive (as defined between GC and Contractor) technological Changes (e.g., new systems or functionality) are introduced into GC environment, in order to facilitate full exploitation of all relevant functional features.	R	A
Provide ongoing training materials for Service Desk personnel on GC business and technical environments as defined by GC.	R	A
Provide classroom facilities for training of GC employees.	I	R

3.8.5.8 Documentation

Documentation Services are the activities associated with developing, revising, maintaining, reproducing and distributing IT Service information in hard copy and electronic form. The following table identifies the Documentation roles and responsibilities, respectively of the Contractor and GC.

Table 49 - IT Life Cycle and Operations – Documentation

Documentation Roles and Responsibilities	Contractor	GC
Recommend Documentation requirements and formats.	R	A
Define Documentation requirements, formats and policies.	C	R
Develop, document and maintain Documentation procedures that meet requirements and adhere to defined policies.	R	A
Review and approve Documentation procedures.	I	R
Provide output in agreed format for support of activities throughout the life cycle of Services as specified in each IT Service.	R	A

Documentation Roles and Responsibilities	Contractor	GC
Maintain and update documentation for system specifications and configurations (e.g., interconnection topology, configurations, and network diagrams). Create documentation when new capabilities or changes are introduced.	R	A
Provide GC-specific operating requirements.	I	R
Document standard operating procedures (e.g., boot, failover, batch processing, backup).	R	A
Review and approve the Standards and Operations Procedures.	I	R
Document job production and maintenance schedules.	R	A
Review and approve job production and maintenance schedules and Documentation.	I	R
Develop a list of standard IT services and products, including standard and available non-standard Equipment and Software configurations and list of services with standard cycle times.	R	A
Review and approve list of standard IT services and products.	I	R
Provide input to GC to support development of a list of in-scope IT services and products, including standard and available non-standard Equipment and Software configurations and list of services with standard cycle times. Maintain the list of products and services as they change.	R	A

3.8.5.9 Incident Management

Incident Management are the activities associated with restoring normal service operation as quickly as possible and minimizing the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. While the Incident Management processes apply to Level 1, Level 2 and Level 3 support groups, Level 1 support — normally at the service desk — is responsible for primary ownership of recording and tracking the Incident.

The Contractor must be responsible for escalating incidents and coordinating with all appropriate Level 2 and Level 3 support groups, to ensure knowledge capture and transfer regarding incident resolution procedures from Contractor's Level 1 service desk to support the objective of increasing the first call resolution number of incidents capable of being resolved by Level 1 service technicians.

The following table identifies the Incident Management roles and responsibilities, respectively of the Contractor and GC.

Table 50 - IT Life Cycle and Operations – Service Support: Incident Management

Service Support: Incident Management Roles and Responsibilities	Contractor	GC
Establish criteria for Incident Management support requirements, including equipment and services to be covered, severity-levels, definitions and characteristics, incident classification prioritization schema, and escalation requirements.	I	R
Develop Incident Management policies, process and procedures that support GC's Incident Management support requirements.	R	A
Review and approve Incident Management policies and procedures.	I	R

Service Support: Incident Management Roles and Responsibilities	Contractor	GC
Provide, maintain, and manage an Incident Management system and knowledge management database, including all Equipment, Software, databases, automated monitoring tools, and management and reporting tools, which are acceptable to GC.	R	A
Provide unrestricted read access by GC-authorized staff and other personnel to all current and historical Incident records and knowledgebase data via a portal.	R	A
Monitor the Incident Management system for automatically generated and logged Incident alerts and events.	R	A
Resolve incidents on the first call in accordance with the Operations and Procedures Manual, knowledge database documents, and configuration database(s).	R	A
Log all calls/queries into the service desk.	R	A
Identify and classify Incidents to a severity level and handle according to agreed-upon Incident response procedures.	R	A
Diagnose and resolve incidents; where possible use Desktop remote-control capability with user's approval and disconnecting when complete. Where possible, implement appropriate corrective actions for known errors (e.g., workarounds for known unresolved Problems). Produce report on remote-control activity.	R	A
Escalate incidents to the appropriate next-level service group within Contractor, GC, or a third-party Service as soon as it is clear that the incident is unable to be resolved without additional assistance or as required to comply with service level response times.	R	A
Monitor and track incident resolution progress through to final closure and record/update incident record status as appropriate.	R	A
Provide expert functional and process assistance for in-scope applications at Level 1 and escalate to Level 2 or 3 resources as required.	R	A
Provide Level 1 assistance to inquiries on the features, functions and usage of Equipment and Software for all in-scope Equipment and Software.	R	A
Provide Level 1 support for applications Software on the supported applications. Level 1 support is limited to approved scripts.	R	A
Provide training and Level 1 scripts for the service desk for applications Software on the approved list.	I	R
Provide Level 2 and Level 3 support for applications Software on the non-supported applications list.	C	R
Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed/resolved incident.	R	A
Assist End Users with questions relating to functionality and use of in-scope Equipment and Software.	R	A
Document solutions to resolved incidents in the central knowledgebase. Accurately update all information pertinent to trouble ticket including general verbiage, codes, etc.	R	A
Notify designated GC personnel of all Severity 1 and Severity 2 incidents within the designated timeframe.	R	A
Maintain current and historical records of all calls and the resolution of those calls for the life of the Contract and provide reporting and trend capabilities.	R	A

Service Support: Incident Management Roles and Responsibilities	Contractor	GC
Troubleshoot, diagnose and resolve incidents for all in-scope Equipment and Software warranty and non-warranty devices, including removing and/or repairing physically broken or inoperable devices.	R	A
Provide Dispatch services for in-scope end point devices and repair as required as per SLRs.	R	A
Provide end-to-end Incident Identification, Escalation and Resolution Management; and a Closure Process including the management of those tickets escalated to third parties.	R	A
Determine wherever possible whether a problem should be opened to address an incident.	R	A
Track ongoing status of any incident and their corresponding problem record to ensure that identified problems are addressed and resolved.	R	A
Ensure incident resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.	R	A
Coordinate and be accountable for incident resolution across all in scope IT service areas with GC and third parties (e.g., public carriers, Internet service Suppliers, third party Suppliers, etc.).	R	A
Periodically review the status of open, unresolved Incidents and related problems and the progress being made in addressing problems.	R	A
Lead Problem Management review sessions.	R	A
Participate in Problem Management review sessions as appropriate.	C	R
Conduct incident review sessions and provide listing and status of same categorized by Incident Severity impact.	R	A
Participate in Incident Management review sessions.	C	R
Coordinate with GC and third-party Level 2 and Level 3 support groups to acquire and transfer knowledge on incident and problem resolutions and record this knowledge gained into the knowledge base to facilitate increased ability for Contractor's Level 1 Service Desk in providing first-call resolution.	R	A
Conduct follow-up with End Users who reported the Incident to verify that the Incident was resolved to the End Users' satisfaction.	R	A
Close out incidents that were resolved satisfactorily.	R	A
Provide Incident Management reporting as required.	R	A

3.8.5.10 Problem Management Services

Problem Management Services are the activities to minimize the adverse impact of incidents and problems on the business, caused by errors within the IT Infrastructure, and to prevent recurrence of incidents related to these errors by determining the unknown underlying cause (e.g., root cause) of one or more incidents. Ensuring that actions are initiated to improve or correct the situation.

The Contractor must provide Problem Management services for all identified problems that are determined to be related to IT systems and services under the control of the Contractor. The Contractor must also provide coordination and assistance to Client and Third-Party Contractor's in performing their Problem Management process.

The following table identifies the Problem Management roles and responsibilities, respectively of the Contractor and GC.

Table 51 - IT Life Cycle and Operations – Service Support: Problem Management

Problem Management Roles and Responsibilities	Contractor	GC
Develop requirements and policies for Problem Management (e.g., events that trigger an RCA, categorization and prioritization schema, etc.).	I	R
Participate in developing Problem Management requirements and policies.	R	A
Develop and implement appropriate process and procedures and methodologies that support GC-approved Problem Management requirements and policies that comply with GC requirements.	R	A
Establish and maintain a Problem Management knowledgebase that is accessible to GC where information about Problems, Root Cause, Known Errors, Workarounds and problem resolution actions are recorded and tracked. This knowledgebase can be the same knowledgebase as used by Incident Management.	R	A
Provide unrestricted read access by GC-authorized staff and other GC designated personnel to all current and historical Problem Management records and knowledgebase data.	R	A
Ensure Problem Management activities conform to defined Change Management procedures set forth in the Standards and Operations Procedures.	R	A
Coordinate with appropriate Incident Management teams and take ownership of Problem Management activities of all problems determined to reside in the Contractor's service area of responsibility (e.g., detection, logging, root-cause analysis, etc.).	R	A
Coordinate, escalate and track Problem Management activities within GC and third parties related to problems determined to reside in all other IT infrastructure areas outside of the Services.	R	A
Flag all incidents that require further root-cause analysis be conducted per the agreed-to procedures.	R	A
Ensure that recurring problems that meet defined criteria are reviewed using root-cause analysis procedures.	R	A
Conduct proactive trend analysis of incidents and problems, and other data elements to identify recurring situations that are or may be indicative of future problems and points of failure.	R	A
Track and report on problems and trends or failures and identify associated consequences of problems.	R	A
Develop and recommend corrective actions or solutions to address recurring incidents and problems, as well as mitigation strategies and actions to take to avert potential problems identified through trend analysis.	R	A
Identify, develop, document, and recommend appropriate Workarounds for known errors of unresolved problems and notify Incident Management and all other appropriate stakeholders of its availability if approved. Document the workaround in the knowledgebase.	R	A
Review and approve Workarounds for implementation, as appropriate.	I	R
Coordinate and monitor status of root-cause analysis activities performed by GC and Third-party Contractor's.	R	A
Document and update Problem Management knowledgebase with information regarding problem resolution actions, activities and status (e.g.,	R	A

Problem Management Roles and Responsibilities	Contractor	GC
root cause, known errors, workarounds, etc.) and notify all appropriate stakeholders of availability of information.		
Coordinate with GC and Third-party service Contractor's to ensure that knowledge on Problems related to other IT service areas is captured and entered into a centralized Problem Management knowledgebase.	R	A
Ensure problem resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.	R	A
Provide status reports detailing the root cause and procedure for correcting recurring, Incidents until closure as determined by GC.	R	A
Conduct Problem Management review meetings and provide listing and status of same categorized by Problem impact.	R	A
Participate in Problem Management review meetings and review and approve recommendations for actions, where appropriate.	C	R
Periodically review the state of open Incidents and related Problems and the progress being made in addressing Problems.	R	A
Participate in and review and approve as appropriate all Problem Management generated Request for Change (RFCs) as part of the Change Management process.	C	R
Create Request for Change (RFC) documentation with recommended corrective actions to be taken to resolve a problem and submit to Change Management for review and approval.	R	A
Conduct monthly problem management proactive review sessions.	R	A
Provide Problem Management reporting as required.	R	A

3.8.5.11 Operations and Administration

Operations and Administration Services are the activities associated with providing a stable IT Infrastructure, and with effectively and efficiently performing procedures to ensure IT services meet SLR targets and requirements. The following table identifies the Operations and Administration roles and responsibilities, respectively of the Contractor and GC.

Table 52 - IT Life Cycle and Operations – Operations and Administration

Operations and Administration Roles and Responsibilities	Contractor	GC
Provide Operations and Administration requirements and policies, including schedules for the operation of GC Service components.	C	R
Develop, document and maintain Operations and Administration procedures that meet requirements and adhere to defined policies.	R	A
Develop operational documentation (i.e., Run Books, Contact Lists, Operations scripts, etc.) that meets GC requirements.	R	A
Review and approve the Standards and Operations Procedures.	I	R
Identify Enterprise System Management tools to monitor the IT infrastructure and GC applications.	R	A
Coordinate with GC to deploy enterprise Service component management tools to monitor the IT infrastructure and GC applications.	R	A

Operations and Administration Roles and Responsibilities	Contractor	GC
Install and configure enterprise Service component management tools in such a fashion that Problems, issues and events are proactively identified, reported and Resolved according to prescribed SLRs.	R	A
Perform event management monitoring of IT Services to detect abnormal conditions or alarms, log abnormal conditions, analyze the condition and take corrective action.	R	A
Manage Equipment, Software, peripherals, Services and spare parts to meet SLRs, minimize downtime and minimize GC resource requirements.	R	A
Manage and coordinate subcontractors and Third Parties in order to meet Service and SLR requirements.	R	A
Develop and provide operational reports and dashboards (e.g., daily, weekly, monthly) that provide status of operational activities, production issues and key operational metrics.	R	A
Review and approve operational reports.	I	R
Audit Operations and Administration policies for compliance with GC policies.	C	R
Provide GC with a copy of or access to any Contract or Third Party-supplied documentation and data (including updates thereto).	R	A

3.8.5.12 Maintenance

Maintenance Services are the activities associated with the maintenance and repair of hardware, software and networks to include "break/fix" Services. Installed platform and product version levels are not to be more than one version behind the current commercial release, unless coordinated with GC architectural standards committee. The following table identifies the Maintenance roles and responsibilities, respectively of the Contractor and GC.

Table 53 - IT Life Cycle and Operations – Maintenance

Maintenance Roles and Responsibilities	Contractor	GC
Define Maintenance standards, requirements and policies.	C	R
Develop, document and maintain Maintenance standards, procedures that meet requirements and adhere to defined policies.	R	A
Develop Maintenance schedules.	R	A
Review and approve Maintenance procedures and schedules.	I	R
Ensure appropriate Maintenance coverage for all Service components.	R	A
Provide maintenance support in GC's defined locations, including dispatching repair technicians to the Service Locations if necessary.	R	A
Perform diagnostics and maintenance on Service components including Equipment, Software, peripherals, Networks and special-purpose devices as appropriate.	R	A
Install manufacturer, service packs, firmware and Software maintenance releases, etc.	R	A
Perform product patch, service pack installation or upgrades to the current installed version where applicable.	R	A
Perform Maintenance-related Software distribution and version control, both electronic and manual.	R	A
Replace defective parts including preventive Maintenance.	R	A

Maintenance Roles and Responsibilities	Contractor	GC
Conduct Maintenance and parts management and monitoring during warranty and off-warranty periods.	R	A
Perform Maintenance Services activities consistent with GC Change Management procedures.	R	A

3.8.5.13 Technology Refreshment and Replenishment

Technology Refreshment and Replenishment (TR&R) Services are the activities associated with modernizing the IT environment on a continual basis, to ensure that the system components stay current with evolving industry-standard technology platforms. The following table identifies the TR&R roles and responsibilities, respectively of the Contractor and GC.

Table 54 - IT Life Cycle and Operations – Technology Refreshment and Replenishment

Technology Refreshment and Replenishment Roles and Responsibilities	Contractor	GC
Recommend TR&R life cycle management policies, procedures and plans appropriate for support of GC business requirements.	R	A
Develop, document and maintain TR&R procedures and develop TR&R plans that meet requirements, adhere to defined policies and Change and Release Management processes.	R	A
Review and approve TR&R policies, procedures and plans.	I	R
Perform the necessary tasks required to fulfill the TR&R plans.	R	A
Provide management reports on the progress of the TR&R plans.	R	A
Periodically review the approved TR&R implementation plans to ensure they properly support GC business requirements.	I	R

3.8.5.14 GC Account Management

Account Management Services are the activities associated with the ongoing management of the Service environment. The following table identifies Account Management roles and responsibilities, respectively of the Contractor and GC.

Table 55 - IT Life Cycle and Operations – Service Support: GC Account Management

GC Account Management Roles and Responsibilities	Contractor	GC
Define GC Account Management requirements and policies.	I	R
Develop, document and maintain GC Account Management procedures that meet requirements and adhere to defined policies.	R	A
Review and approve GC Account Management process and procedures.	I	R
Recommend criteria and formats for administrative, Service activity and Service Level Reporting.	R	A
Review and approve criteria and formats for administrative, Service activity and Service Level Reporting.	I	R
Develop and implement End User Satisfaction Survey program for tracking the Quality of Service delivery to End Users.	C	R
Provide reporting (e.g., statistics, trends, audits).	R	A

3.8.6 Application Service Requirements

3.8.6.1 Corrective and Emergency Maintenance

"Corrective and Emergency Maintenance" refers to repairs to defects so as to enable applications to provide the required functionality and to meet Service Levels, including full recovery of applications, unless otherwise approved by GC, including:

- user interface changes;
- changes to system interfaces;
- application and middleware functional changes;
- recommend database changes related to enhancements;
- modification to standard query structure; and
- report development.

3.8.6.2 Preventative Maintenance

"Preventative Maintenance" refers to the detection and correction (but only where approved by GC) latent faults in applications before they become effective faults, including detecting and correcting events, which if not addressed proactively, could impact applications in production, such as:

- changing business volumes;
- staying on the most current release or as directed by GC;
- application of system patches;
- proactive performance tuning;
- proactive archiving if applicable;
- pre-production execution simulation; and
- special testing for events.

3.8.6.3 Adaptive Maintenance

"Adaptive Maintenance" refers to performing all activities to ensure that application performance and functionality is not adversely affected by a changed or changing environment, including changes to interfacing applications, new applications or packages and technical environment changes, which if not addressed proactively, could impact applications in production, such as:

- providing requirements and supporting upgrades of operating software;
- providing requirements and supporting for new or changed equipment; and
- providing requirements and supporting interfaces, middleware, and application functional and database changes.

3.8.6.4 Perfective Maintenance

"Perfective Maintenance" refers to performing or supporting, as required, all activities (but only where approved by GC) to ensure that applications operate at peak efficiency, including ongoing improvements to application design and operation to improve stability, reliability, and response times

(which may include assessing the bandwidth and the number of users on the system) with particular focus on areas including:

- application performance tuning;
- application response time;
- batch operations; and
- database performance tuning.

3.8.6.5 Applications and Licenses

Application and Licenses are the activities associated with ensuring that product licenses are legally used, and sufficiently available to support relevant GC operations. The following table identifies the applications and licenses roles and responsibilities, respectively of the Contractor and GC.

Table 56 - Applications and Licenses

Applications and Licenses Roles and Responsibilities	Contractor	GC
Maintain licenses for applications, where applicable. This will be under the condition that these licenses are for the sole use of the GC and legally allowed.	R	C
Provide reports of licenses used per application.	R	I
In case of expected license shortages, initiate relevant actions according to the respective Application Services and License Agreements.	R	C

3.8.6.6 Requirements Definition

Requirements Definition are the activities associated with the assessment, definition, verification and validation of user requirements that are used to determine the detailed functional and technical design specifications to realize the gathered, formalized and agreed requirements. The following table identifies requirement definitions roles and responsibilities, respectively of the Contractor and GC.

Table 57 - Requirements Definition

Requirements Definition Roles and Responsibilities	Contractor	GC
Produce SMART (specific, measurable, agreed, realistic and time-bound) requirements for the EPS.	C	R
Document requirements in Requirements Documents.	R	A

3.8.6.7 Design Specifications

Design Specifications are activities that identify and describe the most cost-effective solution to the implementation option under consideration within the limitations of the involved application platforms and or application frameworks. The following table identifies design specifications roles and responsibilities, respectively of the Contractor and GC.

Table 58 - Design Specifications

Design Specifications Roles and Responsibilities	Contractor	GC
Create design specifications that represent the EPS.	R	A

Design Specifications Roles and Responsibilities	Contractor	GC
Verify and validate design specifications that represent the solution to implement the defined requirements.	C	R
Obtain GC's approval for each functional, technical, and security design through coordination with the appropriate respective functional technical application owner for the involved applications.	R	A
Incorporate GC's architectural guidelines into the design, including application extensibility, maintainability, scalability, robustness and reliability.	R	A
Ensure design specifications are aligned to GC security standards.	R	A

3.8.6.8 Software Configuration Management

Software Configuration Management are the activities associated with the identification and maintenance of software components and the relationships and dependencies among them. The following table identifies software configuration roles and responsibilities, respectively of the Contractor and GC.

Table 59 - Software Configuration Management

Software Configuration Management Roles and Responsibilities	Contractor	GC
Perform all software configuration activities that are required as part of the programming and implementation of the programmed solution.	R	A
Ensure all software configuration effort is documented.	R	A

3.8.6.9 Application Development

Application Development relates to activities associated with core and supporting functional Application Development that GC requires from the Contractor.

Table 60 - Application Development

Application Development Roles and Responsibilities	Contractor	GC
Create design specifications that represent the EPS.	R	A
Verify and validate design specifications that represent the solution to implement the defined requirements.	C	R
Obtain GC's approval for each functional, technical, and security design through coordination with the appropriate respective functional technical application owner for the involved applications.	R	A
Incorporate GC's architectural guidelines into the design, including application extensibility, maintainability, scalability, robustness and reliability.	R	A
Ensure design specifications are aligned to GC security standards.	R	A

3.8.6.10 Integration and Testing

Integration and Testing are the activities associated with the functional and non-functional verification and validation of the developed solution at unit and system levels, in interaction with the interfaced applications (including the interfaces). The following table identifies Integration and Testing roles and responsibilities, respectively of the Contractor and GC.

Table 61 - Integration and Testing

Integration and Testing Roles and Responsibilities	Contractor	GC
Perform the following types of testing unless explicitly excluded to verify and validate the programmed solution: • unit testing – the programmed solution modules; • system testing; • integration testing; • regression testing; • load testing; • stress testing; • security testing; and • compliance testing.	R	A
Execute the User Acceptance Tests and Usability Testing as defined by the Contractor as part of the test plan.	C	R

3.8.6.11 Reliability, Availability, Performance, and Security

Reliability, Availability, Performance, and Security relate to activities associated with ensuring Application Services are available within specified parameters, and adhere to strict quality standards, in support of GC service delivery. The following table identifies reliability, availability, performance and security roles and responsibilities, respectively of the Contractor and GC.

Table 62 - Reliability, Availability, Performance, and Security

Reliability, Availability, Performance, and Security Roles and Responsibilities	Contractor	GC
Maintain Application start-up profiles.	R	I
Monitor the Applications for problems and error logs.	R	I
Stop and Start Applications.	R	I
Schedule system housekeeping jobs for system maintenance.	R	I
Provide schedule of system housekeeping jobs for system maintenance.	R	I
Complete daily system (infrastructure) checklist.	R	I
Provide development and configuration objects for migration between environments using standard tools.	R	I
Analyze the system performance at the application system levels.	R	I
Provide application performance targets.	C	R
Recommend appropriate application security measures for adhering to GC policies and regulations.	R	C
Approve application security measures.	I	R
Enact approved application security measures.	R	I
Compare application performance and trends against GC targets.	R	I
Identify and perform first-level analysis of the application performance problems.	R	I
Provide solution for application performance problems.	R	I
Approve identified solution for application performance problems.	I	R
Report application performance.	R	I

Reliability, Availability, Performance, and Security Roles and Responsibilities	Contractor	GC
Maintain Application performance and capacity to meet all Service Level requirements.	R	I
Provide resolution to capacity issues in accordance with GC's approvals.	R	I
Provide GC with reports on capacity when system is nearing capacity limits and propose resolution.	R	I

3.8.6.12 Application Warranty

Application Warranty relates to activities associated with repairing errors/defects for Supplier-developed applications or enhancements that are discovered after application(s) or enhancements are placed into the applicable production environment. The following table identifies Application Warranty roles and responsibilities, respectively of the Contractor and GC.

Table 63 - Application Warranty

Application Warranty Roles and Responsibilities	Contractor	GC
Provide guidance and recommendations on changes to baseline versions in support of Corrective and Emergency Maintenance, and Preventative Maintenance.	R	I
Provide decisions and approval on recommendations for changes to baseline versions.	I	R
Provide all software upgrades/patches/fixes and other change requests as agreed by GC and as documented for Corrective and Emergency Maintenance and Adaptive Maintenance.	R	I
Apply all software upgrades/patches/fixes and other change requests as agreed by GC and as documented for Corrective and Emergency Maintenance and Adaptive Maintenance.	R	I

3.8.6.13 Application Maintenance

Application Maintenance are the activities associated with repairing defects and developing minor functional or technical enhancements for production applications. The following table identifies Application Maintenance roles and responsibilities, respectively of the Contractor and GC.

Table 64 - Application Maintenance

Application Maintenance Roles and Responsibilities	Contractor	GC
Recommend maintenance and repair policies and procedures.	R	I
Approve maintenance and repair policies and procedures as applicable.	I	R
Develop and maintain an Application Maintenance Plan.	R	I
Review and approve Application Maintenance Plan, including any and all revisions to the "Plan" (e.g., committed and proposed work schedules).	I	R
Execute Application Maintenance Plan for all categories of maintenance Services (e.g., Corrective and Emergency Maintenance, Preventative Maintenance, Adaptive Maintenance, and Perfective Maintenance) as described above.	R	I
Provide technical and functional support for the System.	R	I

Application Maintenance Roles and Responsibilities	Contractor	GC
Perform diagnostics on software and services.	R	I
Release and migrate development and configuration objects into production environments using standard tools.	R	I
Confirm successful migration by providing migration logs.	R	I
Review logs and confirm successful migration.	R	I
Recommend appropriate method to migrate objects.	R	I
Review and approve recommendations for migrating objects.	I	R
Develop and recommend configuration management policies and procedures consistent with configuration management practices.	R	I
Review and approve configuration management policies and procedures.	I	R
Perform configuration management activities throughout the development life cycle.	R	I
Maintain and update software configuration information for any changes to be compatible with GC systems.	R	I
Review and approve configuration management results.	I	R
Perform routine system management on applications and middleware as required.	R	I
Perform System configuration maintenance as required.	R	I
Recommend DBMS and middleware tuning changes.	R	I
Provide release packaging of software changes.	R	I
Approve release packaging of software changes.	I	R
Assist the Service Desk with coordination of user support activities.	R	I
Respond to escalated ticket items in accordance with established procedures.	R	I
Follow GC change management procedures associated with maintenance and support.	R	I
Respond to ad hoc GC information requests.	R	I
Provide a comprehensive Disaster Recovery Plan for the System and data in support of GC's requirements.	R	C
Approve the Disaster Recovery Plan for the System application and data.	I	R
Support the communications process via the Service Desk as it relates to the System AMS Services environment.	R	I
Conduct testing prior to User Acceptance Testing.	R	I
Conduct User Acceptance Testing for software patches prior to these patches being promoted to the production environment by Supplier.	I	R
Provide guidance and scripts related to tuning specific components related to the Applications.	R	I
Tune specific components related to the Applications as provided.	R	I
Authorize the migration of objects.	I	R

3.8.6.14 Release Packaging

Release Packaging are the activities associated with the packaging of software changes into suitable releases, by application, as approved by GC. Software version control, both electronic and manual, is included. The following table identifies release packaging roles and responsibilities, respectively of the Contractor and GC.

Table 65 - Release Packaging

Release Packaging Roles and Responsibilities	Contractor	GC
Define release information required for release scheduling and support.	R	I
Define individual release scheduling requirements and interdependencies based on GC provided documentation of business processes.	R	I
Update release information and scheduling requirements and interdependencies in response to changes in GC release needs.	R	C
Identify GC contacts for each production scheduled and on demand release.	I	R
Identify critical releases and define required course of action (e.g., re-start criteria, create incident ticket, etc.), if release fails for production control to follow when monitoring release schedule.	R	I
Provide business requirement for critical release completion timeline and identify action to be taken if release processing is not completed on time.	I	R
Provide analysis and design for specific release schedule for overall release schedule as changes are introduced.	R	I
Test release schedule prior to implementation.	R	I
Approve release schedule design as changes are introduced.	I	R
Schedule and implement releases as per design.	R	I
Provide release process support and trouble shoot job failures, identified by any means, logged from production control.	R	I
Support and monitor release execution as required to ensure release success and timely completion, and identify exceptions.	R	I
Perform analysis and prepare recommendations to fix a problem for failed releases.	R	I
Approve recommendations to correct failed releases.	I	R
Implement approved recommendations to correct failed releases.	R	I
Report errors and re-start failed releases for critical releases following established and documented procedure for critical releases.	R	I
Review logs for critical releases that completed successfully and proactively check for errors that require action. Perform analysis and prepare recommendation to fix a problem for error records logged.	R	I
Identify by any means for release errors that require further support.	R	I
Review logs for non-critical releases and perform necessary steps to resolve problems with non-critical releases. Identify any means that require further support.	R	I
Provide batch process support and trouble shoot release error records based on logged tickets.	R	I
Approve recommendations to be implemented to correct error records within completed releases.	I	R
Implement approved recommendations to correct failed error records within completed releases.	R	I
Manage and maintain release schedule interdependencies, GC's contacts and rerun requirements for all production, test and demand releases in documented form.	R	I

3.8.6.15 Monitoring, Reporting, and Review

Monitoring, Reporting, and Review are the activities associated with the ongoing monitoring (project and application health checks; specific incident, change, problem, project activity tracking; ongoing project and or problem management surveillance), status reporting (project, change, incident, problem, risk mitigation), and review (analysis, escalation, response, resolution of developed policies, procedures, designs, modules, incidents, changes, problems and processes documentation) of application development and or application maintenance activities. The following table identifies monitoring, reporting and review roles and responsibilities, respectively of the Contractor and GC.

Table 66 - Monitoring, Reporting, and Review

Monitoring, Reporting, and Review Roles and Responsibilities	Contractor	GC
Provide an electronic copy of an applications inventory being maintained.	R	I
Provide required reports that capture service requests demands and measure of ability to satisfy demand.	R	I
Provide GC defined reports that represent general health of environments (e.g., number of stranded transports, patches not yet applied) as well as reports that represent demand fulfillment in end-customer terms (e.g., defect corrections/change requests that have slipped against commitment, backlogged defects/change requests).	R	I

3.8.6.16 Troubleshooting and Resolution

Troubleshooting and Resolution are the activities associated with ensuring the provision of adequate technical support, including that the Contractor will diagnose and resolve Incidents as required by failures or deficiencies in previously functioning applications or software, and where required, will make changes to address the failures or deficiencies in previously functioning applications or software (including applying patches, fixes, and updates). The following table identifies troubleshooting and resolution roles and responsibilities, respectively of the Contractor and GC.

Table 67 - Troubleshooting and Resolution

Troubleshooting and Resolution Roles and Responsibilities	Contractor	GC
Provide documentation that clearly identifies the critical business processes and which processes are to be treated as Severity 1 and Severity 2 Incidents.	C	R
Perform diagnosis of all functional and technical Incidents.	R	I
Perform Root Cause Analysis for all Severity 1 and 2 Incidents, or as otherwise requested by GC.	R	I
Perform Root Cause Analysis for Severity 3 and 4 Incidents when requested by GC and or when deemed required by Problem Management.	R	I
Perform problem management and escalation in accordance with the GC problem management process.	R	I
Escalate to Contractor or Level 3 Third Party vendors if required.	R	I
Monitor vendor for patch/fix/updates – escalate if required.	R	I
Perform Corrective and Emergency Maintenance.	R	I
Perform Adaptive Maintenance.	R	I

Troubleshooting and Resolution Roles and Responsibilities	Contractor	GC
Document and promptly notify GC and Third Party Vendors of any emergency changes.	R	I
Resolve, perform unit testing, functional testing and support GC and Third Party Vendors User Acceptance Testing as applicable, and apply desired resolution for activities specific to Level 2 and Level 3 Support and provide Corrective and Emergency Maintenance.	R	I
Provide existing automated regression testing scripts for activities specific to Adaptive Maintenance.	R	I
Maintain automated regression testing scripts.	R	I
Maintain and update user test scenarios/test cases.	R	I
Conduct User Acceptance Testing as required.	I	R
Support User Acceptance Testing.	R	I
Validate the installation of the EPS into the production environment. Validation activities include executing functionality delivered within production environment and confirming results meets agreed to acceptance criteria.	R	I
Review and approve successful installation of the solution into the production environment as required.	I	R
Follow GC change management process for introducing change into the production environment.	R	I

3.8.6.17 Artifact Management

Artifact Management relates to activities associated with maintaining all artifacts needed to support GC applications, including updating such artifacts based on changes initiated by GC. The following table identifies Artifact Management roles and responsibilities, respectively of the Contractor and GC.

Table 68 - Artifact Management

Artifact Management Roles and Responsibilities	Contractor	GC
Maintain artifacts for configuration design and source code management, system/business requirements, functional specification, technical design, regression test plan, unit test plans, functional test plans, custom code components and batch schedule.	R	I
Maintain artifacts for architecture standards, business architecture, logical database design, security architecture model and User Acceptance Test plans.	I	R
Maintain artifacts for technology architecture.	I	R
Maintain artifacts for, physical database structure, application security implementation design.	R	I
Update artifacts based on changes in the environment as appropriate and as requested.	R	I
Provide full access to GC to view and review artifacts at all times.	R	I

3.8.6.18 User Management

User Management Relates to activities associated with implementing and executing the approved processes and procedures for the control of System security, including the creation and maintenance

of system security profiles and user profile configuration for groups who are using the System. The following table identifies User Management roles and responsibilities, respectively of the Contractor and GC.

Table 69 - User Management

USER MANAGEMENT ROLES AND RESPONSIBILITIES	Contractor	GC
Form and develop associated user profile requirements in accordance with GC policies and procedures.	I	R
Reset passwords as required for development, system integration testing, training and patching sustainment environments for Supplier System team.	R	I
Responsibility for Internal/External users' security requirements.	I	R
Create user ids.	R	I
Lock/unlock User IDs as required for all environments.	R	I
Disable, terminate and purge user profiles upon request for all environments.	R	I
Ensure the solution includes all necessary design elements required to support user profile scalability.	R	A

3.8.7 IT Service Levels

3.8.7.1 Application Availability

This service level measures the availability of the systems and their various components.

Table 70 - Application Availability

APPLICATION AVAILABILITY			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	The percentage of time that the application is available for normal business operations.	Production Applications: 99.5% Non Production Applications: 95.00%
	Formula	[Number of hours during the month being report on when the production applications and their various components were operating without any Severity Level One or Two incidents] divided by [Total number of hours during such month minus (number of hours of maintenance window + planned downtime)] multiplied by 100 = [percentage of availability of the application during such month].	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data.	

3.8.7.2 Planned Maintenance Window and System Downtime

This service level measures the maximum acceptable time for planned maintenance and system downtime activities for production systems.

Table 71 - Planned Maintenance Window and System Downtime

PLANNED MAINTENANCE WINDOW AND SYSTEM DOWNTIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	The percentage applications that meet planned maintenance window and downtime schedule requirements.	Production Applications: 100% Non Production Applications: 95.00%
	Formula	[Number of applications that adheres to the planned maintenance window and downtime schedules] divided by [Total number of applications] Multiplied by 100 = [percentage of applications that meet planned maintenance window and downtime schedule requirements per month]	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.3 Transaction Response Time

This service level measures the time elapsed from the instance a User enters a command or query within an application until the requested information, query result, report, etc. is returned to the User.

Table 72 - Transaction Response Time

TRANSACTION RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	The percentage of transactions that meet response time performance requirements of 2.8s.	Production Applications: 99.00%
	Formula	[Number of transactions completed within the target time frame] divided by [Total number of transactions within the measurement period] multiplied by 100 = [percentage of transactions that meet response time performance requirements in such day].	
	Measurement Interval	Daily	
	Reporting Period	Weekly	
	Measurement Method/Source Data	TBD	

3.8.7.4 Software Management – Notification of Available Patches, Updates, and Releases

This service level measures the timeliness of notifying the client about the availability of patches, service packs, updates and new releases across all applications, data bases, middleware and tools.

Table 73 - Software Management – Notification of Available Patches, Updates, and Releases

SOFTWARE MANAGEMENT – NOTIFICATION OF AVAILABLE PATCHES, UPDATES, AND RELEASES			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	The percentage of events notified within the target time frame: Patches: Within 5 Business Days after vendor announcement Other Updates: Within 30 Calendar Days after vendor announcement	Patches: 99.00% Other Updates: 95.00%
	Formula	[Number of events notified within the target time frame] divided by [Total number of events in the measurement period] multiplied by 100 = [percentage of events notified within the target time frame during such month].	
	Measurement Interval	Quarterly	
	Reporting Period	Quarterly	
	Measurement Method/Source Data	TBD	

3.8.7.5 Software Management – Implementation of Patches, Updates, and Releases

This service level measures the timeliness of implementing patches, service packs, updates and new releases across all applications, data bases, middleware and tools.

Table 74 - Software Management – Implementation of Patches, Updates, and Releases

SOFTWARE MANAGEMENT – IMPLEMENTATION OF PATCHES, UPDATES, AND RELEASES			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	The percentage of events implemented per client-approved schedule	99.00%
	Formula	[Number of events implemented within the target time frame] divided by [Total number of events in the measurement period] multiplied by 100 = [percentage of events implemented within the target time frame such month].	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	

SOFTWARE MANAGEMENT – IMPLEMENTATION OF PATCHES, UPDATES, AND RELEASES		
	Measurement Method/Source Data	TBD

3.8.7.6 Runbook Change Timeliness

This service level measures the timeliness of executing Runbook changes required by the client.

Table 75 - Runbook Change Timeliness

RUNBOOK CHANGE TIMELINESS			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	All applications changes are executed in line with GC approved schedule.	100.00%
	Formula	[Number of all Runbook changes executed within the target time frame for each type Application] divided by [Total number of all Runbook changes for each type of Application] multiplied by 100 = [percentage of all Runbook changes executed within the target time frame such month].	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.7 Runbook Change Accuracy

This service level measures the accuracy of the Runbook changes compared to client-approved requirements.

Table 76 - Runbook Change Accuracy

RUNBOOK CHANGE ACCURACY			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	All applications changes are accurate compared to client-approved requirements.	100.00%
	Formula	[Total number of Runbooks that are changed in accordance with CLIENT-specified requirements] divided by [Total number of Runbooks changed] multiplied by 100 = [percentage of Runbook Accuracy such month].	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	

RUNBOOK CHANGE ACCURACY		
	Measurement Method/Source Data	TBD

3.8.7.8 Enhancement Request Response Time

This service level measures the timeliness of responding to enhancement requests with an estimate and proposal that is compliant with defined standards and requirements.

Table 77 - Enhancement Request Response Time

ENHANCEMENT REQUEST RESPONSE TIME			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Contractor responds to client requests within 10 business days.	95.00%
	Formula	[Number of enhancements with estimates and proposals submitted within target time lines and compliant with client-defined standards and requirements] divided by [Total number of enhancements in the measurement period] multiplied by 100 = [percentage of enhancements where Contractor is responsive to client requests within such quarter].	
	Measurement Interval	Quarterly	
	Reporting Period	Quarterly	
	Measurement Method/Source Data	TBD	

3.8.7.9 Cost Estimate Adherence

This service level measures the adherence to cost estimates for enhancements provided.

Table 78 - Cost Estimate Adherence

COST ESTIMATE ADHERENCE			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Actual cost ranges from 90% to 110% of the original cost estimates.	95%, with no enhancement more than 125% of the original cost estimates.
	Formula	[Number of enhancements with actual costs within the acceptable deviation limits vs. the original cost estimates] divided by [Total number of enhancements in the measurement period] multiplied by 100 = [percentage of enhancements where the Contractor has	

COST ESTIMATE ADHERENCE		
		adhered to cost estimate adherence requirements within such quarter].
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.8.7.10 Schedule Adherence

This service level measures the adherence to schedule estimates for enhancements provided.

Table 79 - Schedule Adherence

SCHEDULE ADHERENCE			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	Actual schedule ranges from 90% to 110% of the original schedule estimates.	Critical Milestones: 100% completed on or before the original milestone date Other Milestones: 90% completed on or before the original milestone date
	Formula	[Number of enhancements with achievement of milestones within the acceptable deviation limits vs. the original milestone dates] divided by [Total number of enhancements in the measurement period] multiplied by 100 = [percentage of enhancements where the Contractor has adhered to schedule adherence requirements within such quarter].	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.11 Network Availability

Network availability is the parameter to measure the availability of data network components. Measures include WAN, LAN, and VPN availability.

Table 80 - Network Availability

NETWORK AVAILABILITY			
Component	Service Measure	Performance Target	SLR Performance %

NETWORK AVAILABILITY			
Network	Minutes of Uptime	100% uptime	WAN/LAN Availability: ≥ 99.5 % VPN Availability: ≥ 99.5 %
	Formula	[(Actual Uptime plus Excusable Downtime during the Measurement Interval) divided by (Scheduled Hours during the Measurement Interval)] multiplied by 100 %] = [percentage of Availability of the Network components]	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.12 Network Performance (Latency)

Parameter to measure the transit delay (in elapsed time) from ingress and egress ports on premise devices.

Table 81 - Network Performance (Latency)

NETWORK PERFORMANCE (LATENCY)			
Component	Service Measure	Performance Target	SLR Performance %
Network	Transit delay in ms	N/A	Performance < 50 ms
	Formula	t2 minus t1 = Network Transit Delay (NTD) Where: t1 = the time when a packet leaves the egress premise, t2 = the time when the packet arrives at the ingress premise	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.13 Packet Delivery Ratio

The Packet Delivery Ratio is the parameter to measure rate of successfully packet transmission.

Table 82 - Packet Delivery Ratio

PACKET DELIVERY			
Component	Service Measure	Performance Target	SLR Performance %
Network	Percentage of successful packet transmissions	N/A	≥ 99.5 %
	Formula	(total packets delivered during the Measurement Interval) divided by (total packets sent during the Measurement Interval) = Packet Delivery Ratio (PDR)	

PACKET DELIVERY		
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.8.7.14 Solution Currency (n-1 version)

This refers to the EPS components to be managed proactively using product-specific monitoring and management tools.

Table 83 - Solution Currency (n-1 version)

SOLUTION CURRENCY (N-1 VERSION)			
Administrative Task	Service Measure	Performance Target	SLR Performance %
Implementation of service packs and updates to "dot" releases	Response Time	Within 60 days after approved by GC	95.0%
Implementation of version or major release updates	Response Time	As per approved project plan	95.0%
	Formula	[Number of tasks required to be performed by the Contractor during the Measurement Interval and completed within Target Performance] divided by [Total of all tasks required to be performed by Contractor during Measurement Interval] times 100 % = [Percent (%) Attained]	
	Measurement Interval	Monitor Continuously, Measure Daily	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.15 Capacity Management: Number of Incidents Caused by Inadequate Capacity

This is the parameter to measure the percentage of all Service Desk incidents related to capacity issues.

Table 84 - Capacity Management: Number of Incidents Caused by Inadequate Capacity

CAPACITY MANAGEMENT: NUMBER OF INCIDENTS CAUSED BY INADEQUATE CAPACITY			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	% of incidents logged with the Service Desk that were caused by lack of capacity	5%

CAPACITY MANAGEMENT: NUMBER OF INCIDENTS CAUSED BY INADEQUATE CAPACITY		
	Formula	[Number of Service Desk incidents related to capacity issues and logged during the Measurement Interval] divided by [total number of Service Desk incidents logged during the Measurement Interval] times 100 % = "Percent (%) Capacity-Related"
	Measurement Interval	Monthly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.8.7.16 Capacity Management: Capacity Utilization – Memory

This is the parameter used to measure the capacity utilization of available memory resources by the applications, data bases and middleware, for each processor used to support the applications.

Table 85 - Capacity Management: Capacity Utilization – Memory

CAPACITY MANAGEMENT: CAPACITY UTILIZATION – MEMORY			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	% of memory capacity utilized during the reporting period to support the EPS application	Median Usage: 50.00% Peak Usage: 70.00%
	Formula	[Memory usage across each processor] divided by [Total available processor capacity] multiplied by 100 = [percentage of memory capacity utilized during such day]	
	Measurement Interval	Daily	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.17 Capacity Management: Capacity Utilization - Storage

This is the parameter used to measure the capacity utilization of available production storage resources by the applications, data bases and middleware, across all infrastructures used to support the applications.

Table 86 - Capacity Management: Capacity Utilization - Storage

CAPACITY MANAGEMENT: CAPACITY UTILIZATION – STORAGE			
Application	Service Measure	Performance Target	SLR Performance %
EPS	Percentage	% of storage capacity utilized during the reporting period to support the EPS application	Peak Usage: 80.00%

CAPACITY MANAGEMENT: CAPACITY UTILIZATION – STORAGE		
	Formula	[Total production storage used] divided by [Total production storage capacity] multiplied by 100 = [percentage of storage capacity utilized during such week]
	Measurement Interval	Weekly
	Reporting Period	Monthly
	Measurement Method/Source Data	TBD

3.8.7.18 Capacity Management: Data Network Service Capacity Reallocation or Change

As a result of proactive monitoring, the parameter to measure pre-emptive intervention to advise GC of the need to increase capacity.

Table 87 - Capacity Management: Data Network Service Capacity Reallocation or Change

CAPACITY MANAGEMENT: DATA NETWORK SERVICE CAPACITY REALLOCATION OR CHANGE			
Component	Service Measure	Performance Target	SLR Performance %
Network	Percentage of time GC has been successfully notified of network capacity threshold breach	Upon sustained average daily utilization of Data Network service capacity reaching or exceeding 60% of installed capacity, Contractor must notify GC within one elapsed day of the over 60% utilization situation.	≥ 99 %
	Formula	[Number of tasks required to be performed by the Contractor during the Measurement Interval and completed within Target Performance] divided by [Total of all tasks required to be performed by the Contractor during the Measurement Interval] times 100 % = [Percent (%) Attained]	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

3.8.7.19 Capacity Management: Network Capacity Addition or Change

This is the parameter to measure the timely completion of each increase or decrease in capacity as scheduled under the change management process. Time is measured upon approval by GC of the change.

Table 88 - Capacity Management: Network Capacity Addition or Change

CAPACITY MANAGEMENT: NETWORK CAPACITY ADDITION OR CHANGE			
Component	Service Measure	Performance Target	SLR Performance %
Network	Number of scheduled capacity increase implementations	The Contractor will complete each increase of capacity scheduled under the change management process within 30 elapsed days of approval by GC and each decrease of capacity scheduled under the change management process within 3 calendar months of approval by GC.	≥ 95 %, 100%of increases in installed capacity within 2 months 100% of decreases in installed capacity within 4 months
	Formula	[Number of tasks required to be performed by the Contractor during the Measurement Interval and completed within Target Performance] divided by [Total of all tasks required to be performed by the Contractor during the Measurement Interval] times 100 % = [Percent (%) Attained]	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

PART 4: TECHNICAL REQUIREMENTS

4.1 INFORMATION TECHNOLOGY AND SOLUTION MAINTENANCE AND UPDATES

4.1.1 Baseline Solution

The Contractor must deliver, enable, and maintain a core solution including relevant information technology hardware and software components and related business processes to deliver the core functional requirements detailed in the SOW. The core baseline information technology solution must be able to accommodate the modification, adjustment, or addition of business process work flows, system automated functions, and other related procurement management rules and processes without application code changes related to the delivery of EPS under this Contract. The core solution must include management and operations support of the scalable, robust, resilient On-demand computing and network infrastructure.

4.1.2 Continuous Technology Improvement to Baseline Solution

The Contractor must maintain and update hardware, software, and other related IT solution components of their core solution in support of the functional requirements under this Contract. Continuous improvement includes keeping these solution components current (i.e. software updated releases and evergreen hardware cycle upgrades), compatible with changing GC standards and relevant to common industry practices for the same types of service delivery. Continuous improvement requirements will require the Contractor to employ software, hardware, and other related technology solution components that are versatile and can functionally interact and integrate with IT components used by delivery partners and that are common within managed service arrangements, as may be updated and modified during the life of this Contract.

4.1.3 Change Management - Addition of New Technology Components

The Contractor must deploy a solution that is flexible, scalable, adaptable and commercially available which will result in minimal enhancement costs to GC.

4.2 HARDWARE REQUIREMENTS

GC will procure a secure hosted managed service for the EPS. No installation of hardware, other than Network connectivity pieces, upon GC premises will be considered or permitted for the purpose of this procurement.

The Contractor must provide, develop, configure, test, maintain and house all infrastructure in its premises to support the solution deployed to meet all the requirements defined in the SOW. The Contractor must monitor and conduct quality assurance tests on the hardware in place, and incorporate hardware updates as required to ensure the hardware capabilities meet the output demand of the overall solution.

4.3 SOFTWARE REQUIREMENTS

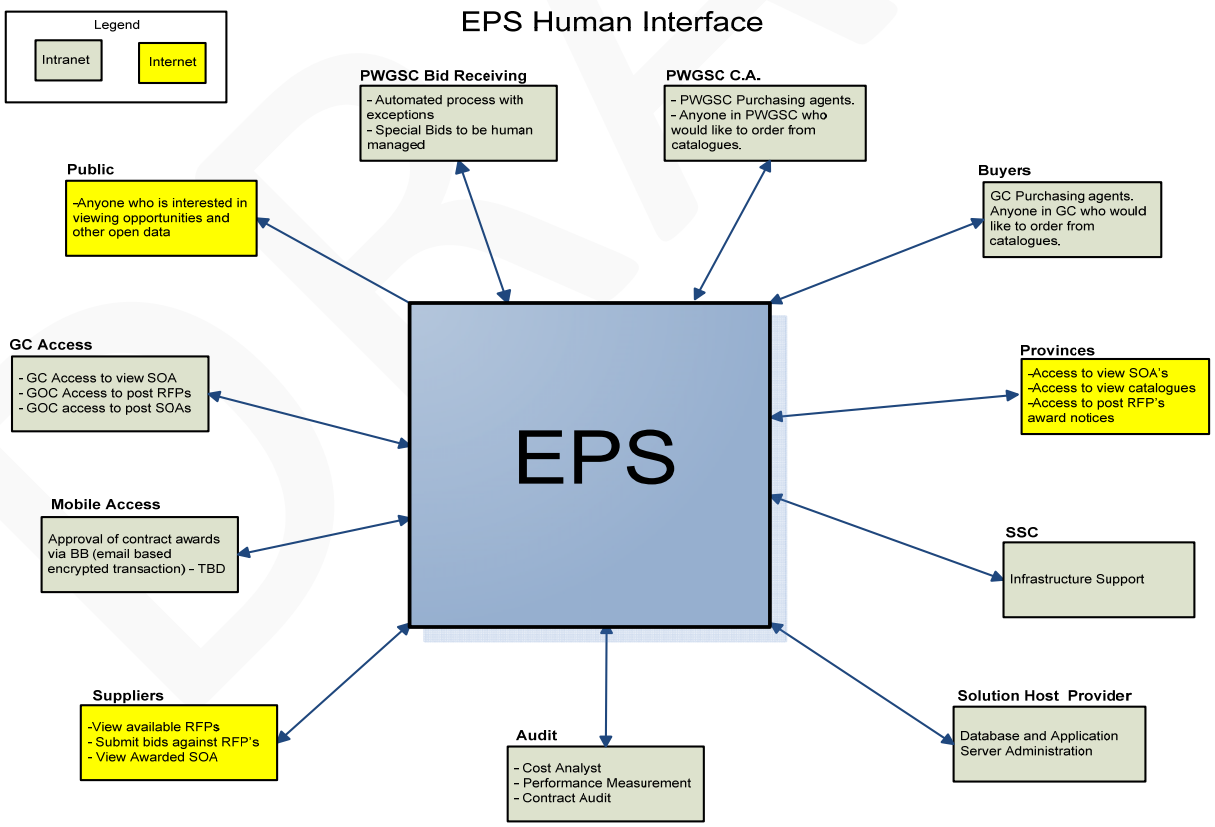
The Contractor must deliver, enable and maintain software solutions that are flexible, adaptable and scalable in order to accommodate any changes to the requirements over time or any increase in processing volumes (e.g. automated business processes, changes to business rules, enhanced services). In order to support these requirements, GC is expecting the EPS to have been built on N-Tier application architecture pattern. There must be clear separation of user interface, application logic and data, in order to allow flexibility in the design. Components must be loosely coupled for easier and faster maintenance and upgrade of the application, as well as quicker deployment and management of components and services.

The EPS must have a capability of modular architecture, Service Oriented Architecture (SOA), so as to have the ability to rapidly respond to changing functional requirements and, or channel needs.

4.4 DELIVERY PARTNER ACCESS TO THE SYSTEM/DATA

The following diagrams depict an overview of the business use cases and system to system interfaces associated with the EPS. Roles and functions of each use case are described in the Security Classification Guide as a part of this RFP, and the requirements for system interfaces are detailed in Section 4.5 Interfaces with Government of Canada Systems of this SOW.

Figure 3 - EPS Human Interface



4.5 INTERFACES WITH GOVERNMENT OF CANADA SYSTEMS

4.5.1 Background

In the context of EPS, the GC Interface is the capability for people, process and technology working together efficiently to ensure that the right procurement data is available to the right people in order to deliver responsive and cost effective procurement services in a timely manner. In order to develop and support such streamlined procurement services, the EPS is required to exchange information with procurement support systems and other back-office systems.

This section describes the data exchange requirements for EPS and related technical requirements based on current information. Its purpose is:

- To ensure that the EPS aligns with GC standards and facilitates interoperability with GC and/ or PWGSC target suites, GC back-office systems, processes and data; and
- To identify and specify the high level data exchange requirements with other departmental systems and non-GC data sources.

The Technical Requirements in section 4.6 specifies applicable technology standards, policies, directives and requirements in support of these data exchange requirements in this section.

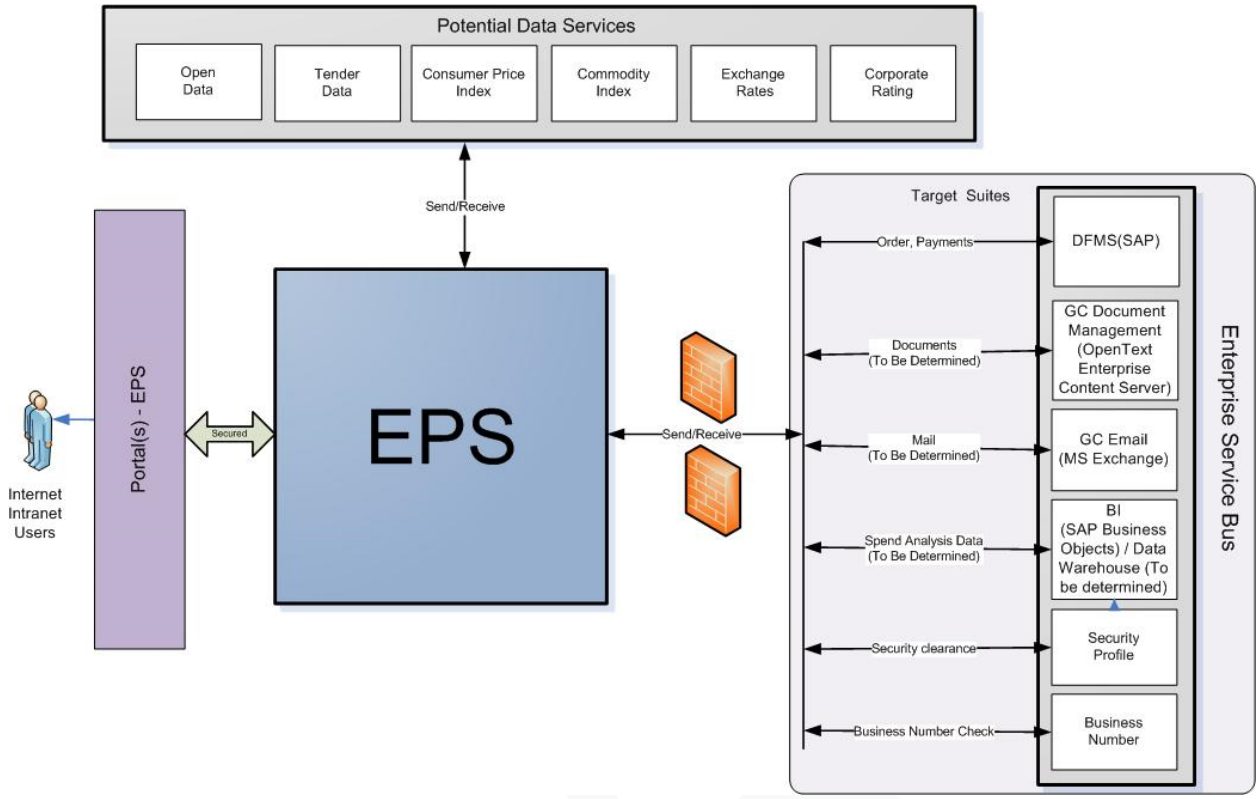
The PWGSC standard tool for interoperability between back office systems and business processes is the Oracle Enterprise Service Bus (ESB). While the standards and methods for ESB integration are being defined as a part of the ESB rollout project, Simple Object Access Protocol (SOAP) based messages and/or file exchanges are planned to be supported.

The end-state of EPS must be fully aligned with the GC Financial Management Transformation (FMT) initiative, and to provide the key technology capability in support of GC's streamlined financial management processes. Under the FMT strategy, EPS may be utilized as the only sourcing and procurement solution for all departments and be integrated with existing enterprise back-office systems, such as Departmental Financial Materiel Management Systems (DFMS).

4.5.2 Solution Vision

Figure 4 depicts an end-state vision of data exchange between EPS and other systems. The EPS is envisioned to be a key component of GC wide procure-to-pay process. As such it will be connected to a number of procurement process support systems and will need to interoperate with Departmental Finance Materiel Management Systems (DFMS). The EPS must also support GC's open data initiative by aggregating and posting procurement data to Open.canada.ca. Detailed requirements for each interface are provided further in this section.

Figure 4 - EPS Vision



4.5.2.1 Dependencies

Enterprise IT Target Suites These target suites are driven by both Chief Information Officer (CIOB) Branches in Treasury Board Secretariat of Canada (TBS) and PWGSC to rationalize and standardize the application footprint. Where applicable, the EPS will be dependent on government direction, which includes: OpenText Enterprise Content Server (Document Management System); Departmental Financial and Materiel Management Systems (DFMS-SAP); GC e-mail (Microsoft Exchange); Business Intelligence (SAP Business Objects); and Oracle Enterprise Service Bus (ESB).

GC Financial Management Transformation (FMT) As well, the EPS will be dependent on the standards established under the TBS Common Enterprise Data Initiative (CEDI) which includes Procurement, Vendor and Financial data.

4.5.2.2 General System Interoperability

There is a requirement for structured and modular external interfaces which will allow information exchange between the EPS and other business / financial systems through a secure communications infrastructure.

These interfaces include, but are not limited to:

- An intranet or extranet for the key business processes described in Business Requirement Document.
- Web services – third party data feeds.

- Commercially available third party security components such as Public Key Infrastructure (PKI) products.
- Other procurement systems to transmit and receive information.
- Other systems containing product information that capture this information for use within its solution.
- Systems containing supporting information needed to process transactions.
- Commercially available financial and materiel systems (FMS) using generic pre-built adapters that facilitate the interface with SAP.

The Contractor must supply a list of all interfaces affected and 3rd party application interoperability modules and/or application programming interfaces (API) used in the solution. The Contractor must ensure these APIs are interoperable with GC's standard platforms.

The Contractor must provide an application integration toolkit that GC partners can leverage for support in creating integration methodologies, if needed, for their applications that includes:

- Enterprise Application Integration tool in a media and format specified by GC.
- reference documentation (in English and French) on tool usage that includes:
- Original Equipment Manufacturer (OEM) manuals and guides;
- instructional documents providing details on controls, methods, data dictionaries, etc.;
- best practices and whitepapers;
- sample application integration source code;
- a list of all libraries supported by the service;
- an application compliance testing guide that includes:
- test cases that GC partners can use to assess an application's compliance with supported protocols and standards; and
- a compliance checklist that GC partners can complete to record and report on compliance testing results.

4.5.2.3 Technical Interoperability

The EPS must interoperate with GC's IT stack (i.e. infrastructure and platform) without significant change to the existing GC infrastructure or changes to desktops.

The following is a list of types of expected technologies that must be supported:

- Open ID connect
- SAML 2.0
- JSON
- Kerberos
- X.509
- LDAP
- ABAC
- OAuth
- SOAP

- REST

4.5.2.4 Interoperability with GC Back-Office Systems

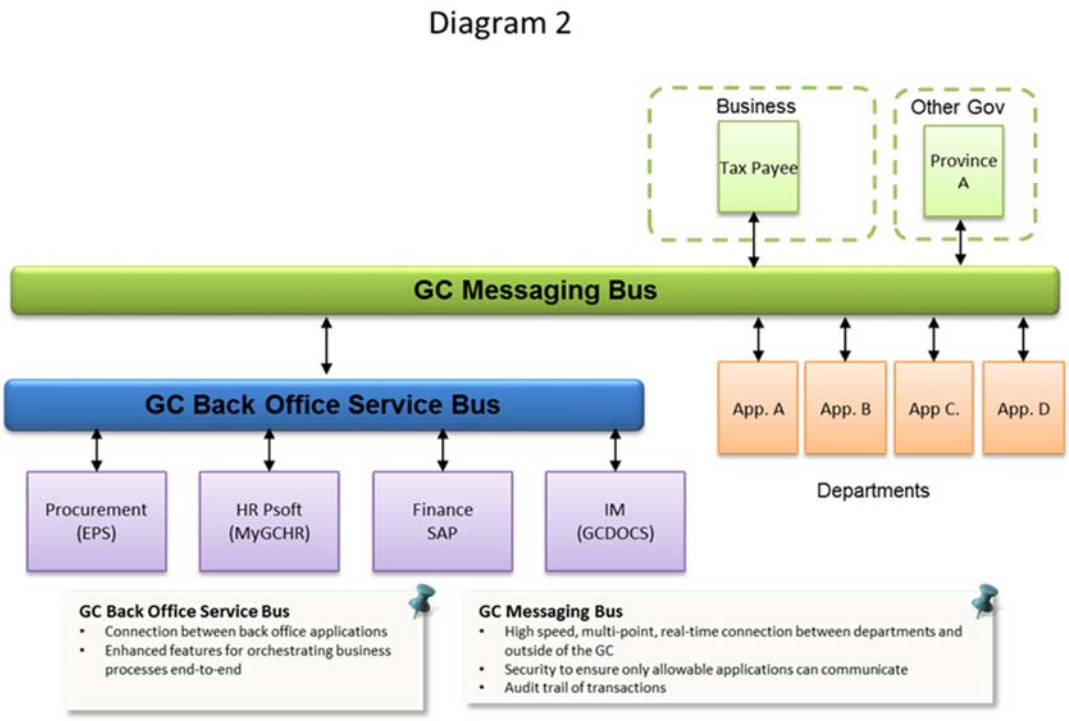
In support of Canada's strategic plans for application interoperability, the proposed e-Procurement solution must expose its functionality through an Application Programming Interface (API) that leverages industry-standard API protocols. Functionality to be exposed includes the following:

- Ability to create/read/update/delete business objects in the e-Procurement solution
- Ability to invoke/trigger business processes within the e-Procurement solution
- Ability to publish business object and contract lifecycle related events using near real-time messaging

GC is in the process of developing a universal application bus, known as Enterprise Service Bus (ESB), that will become the new interface standard. The new service bus will be standardized on Oracle ESB technology platform, including its Business Process Management (BPM) solutions. The technology standards expected to be used are JMS (RFC 6167) and XML.

The following Figure 5 depicts a high level vision of ESB. The GC Back Office Service Bus depicted below is where EPS will be positioned and is part of a wider context established by the Treasury Board Secretariat of Canada (TBS) and known as *the Government of Canada Interoperability Framework* (GCIF).

Figure 5 - High Level Vision of ESB



4.5.2.5 Requirements for Government Interfaces

The following sections describe the interface requirements in two different states; : the Pre-FMT state is defined as the period from the EPS rollout to the beginning of Financial Management Transformation (FMT) implementation and; the Post-FMT state is a period where the role of EPS is more clearly defined in terms of GC's P2P process.

4.5.2.6 EPS Requirements – Pre-FMT Implementation

Table 89 - Pre-FMT Implementation

SOW NUM	Requirement
Pre.00	**Pre-FMT Implementation - Departmental Financial Materiel Management System (DFMS)** The Contractor must deliver a solution that provides the functionality:
Pre.01	to create and send a Purchase Order(P/O) to suppliers from EPS via notifications(email or alerts on the portal). P/O outlines the Order item details, supplier information, plus Terms and Conditions (T&C), delivery information.
Pre.02	to interface with DFMS, for SAP instances only, in real-time using the approved interoperability technology, such as ESB or APIs, using XML to support the integrated procurement processes:

SOW NUM	Requirement
	• sending the purchase order(P/O) to DFMS; and • receiving the goods receipt, invoice and payment records from DFMS.
Pre.03	to transfer data to the e-Tendering portal using ESB or Web services.
Pre.04	to transfer structured and unstructured data to Open Government Portal.
Pre.05	to support dynamic access to open data datasets, within e-Tendering and Open Government Portal, thru API calls as services.
Pre.06	to support open tender data for all Canadian Public Sectors by aggregating, posting and updating the tender notices in any file format from other jurisdictions.
Pre.07	to support Extract, Transform and Load (ETL) processes between EPS's own BI/Data Warehouse and GC's corporate BI (SAP Business Objects)/Data Warehouse (To Be Decided) in batch/real-time mode.
Pre.08	to support the validation of supplier's business number and legal name in real-time using XML with the CRA's Business Number Hub system.
Pre.09	to receive the exchange rates in real-time for specified currencies, from the designated source (e.g. Bank of Canada).
Pre.10	to receive Consumer Price Index (CPI) data from Statistics Canada in real-time.
Pre.11	to receive the commodity index feed from Bank of Canada, and/or other designated sources in real-time.
Pre.12	to receive security clearance data in real-time on both corporate and resource level from CISD (Canadian Industrial Security Directorate).
Pre.13	to receive the supplier's corporate rating in real-time, from designated source(s), e.g. Dunn and BradStreet.
Pre.14	to support data exchanges to and from legacy systems during the transitional period using GC preferred interface frequency, styles and methods: • real-time or batch • Web services / APIs • XML and/or Flat file.

4.5.2.7 EPS Requirements – Post FMT Implementation

Table 90 - Post FMT Implementation

SOW NUM	Requirement
Post.00	**Post-FMT Implementation - Departmental Financial Materiel Management System (DFMS)** The Contractor must deliver a solution that provides the functionality:
Post.01	to integrate with all DFMS instances (SAP) in real time utilizing the standard data and process integration tool (Oracle Enterprise Service Bus and BPEL).

SOW NUM	Requirement
Post.02	to use the Spend categorization schema defined by CEDI/FMT for spend analysis.
Post.03	to integrate with new GC common business number Hub system, via ESB, for all supplier tombstone data.

4.6 EPS TECHNOLOGY REQUIREMENTS

4.6.1 Introduction

It is envisioned that the EPS will be comprised of a Contract Management Solution (sourcing, supplier relationship management and contract life-cycle management) and an e-Catalogue Solution. The EPS, however, must be a Software as a Service (SaaS) solution which meets or exceeds the core business functional requirements specified in this SOW. EPS must also be a flexible, scalable and adaptable solution that meets changing business needs mostly through managing configurations available within the solution.

The bidders must demonstrate their solution's capabilities and maturity by submitting the following artefacts and plans as part of the proposal. The following submitted documents are required to evaluate the overall technical capabilities, soundness and long-term viability of the solution as a whole.

1. Architectural diagrams, at both the conceptual and logical level, of the overall solution being proposed. The architecture diagrams must address the business, application, integration, data, security and technology perspectives.
2. Scalability and performance management plans that show how scalability and performance will be addressed to meet the SLAs in the SOW.
3. Information management plan that describes the data and how it will be managed; a high level data flow among the logical functional components.
4. A list of pre-build APIs for integration with ERPs and other data sources defined in the GC interfaces section.
5. A description of the SaaS model being proposed.

The technical requirements in this section describe what the solution must be able to deliver, enable and support in terms of technical capabilities that must be met for the solution to co-exist and interoperate with other GC systems.

There are four key areas addressed in this section:

- Compliance
- Interoperability
- Usability
- Reliability

4.6.1.1 Compliance

The AP is governed by broader legislation, regulations, and policies to which the Contractor must adhere. Ensuring the security and protection of personal and corporate information remains a priority for the GC and all solutions and processes must adhere to all relevant legislation including but not limited to those related to privacy and the handling and storage of information.

Compliance requirements in this section are technology specific requirements the Contractor must follow.

4.6.1.2 Interoperability

Interoperability is the ability for people, process, and technology to work together efficiently to ensure that the right information is available to the right people or system at the right time.

The EPS must be able to interoperate with GC's applications and platforms using as a minimum the following: 1) APIs; 2) Export and import of data and content; and 3) Enterprise Messaging/Service Bus.

Interoperability enables an enterprise's capability to exchange information within itself and with other enterprises with the intent to achieve greater operational efficiencies and more effective outcomes. The GC is developing a GC Interoperability Framework (GCIF). The objective is to align to and support the Whole-of-Government Framework approach to planning, designing, operating and managing GC programs and services on an enterprise-wide basis.

4.6.1.3 Usability

Usability refers to the ease of use and learn-ability of the solution. The usability requirements in this section focus on GC and IT industry best practices and standards that have been adopted widely for building and maintaining the easy-to-use Web applications.

4.6.1.4 Reliability

Requirements in this category specify solution capabilities and architecture that in general give a higher level of availability, more maintainable application (i.e. easy to add features, functions etc.), and higher overall resiliency.

Please note: The versions and particular brand names are provided when the information is available. As with all other GC policies and standards, the technology standards change and EPS is expected to support the technology standard changes as required and when GC is ready.

4.6.2 Technical Requirements

Table 91 - General Requirements

SOW NUM	Requirement
Tech.00	**Technical Requirements** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
Tech.01	to comply with GC policies and standards and comply with regulations applicable to GC including information systems, personnel, physical and technical security. https://www.cse-cst.gc.ca/en/publication/list/IT-Risk-Management.
Tech.02	to align with the Directive on Open Government requirements in the following link, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28108, as it pertains to EPS's needs to transfer selected procurement data to open data portal for public.
Tech.03	to be interoperable with GC's applications and platforms using at least the following methods: - APIs; and - export and import of data and content; and - Enterprise messaging/Service Bus.
Tech.04	to support the concept of open architecture and allowing accessibility to its services and functionalities through other vendor-provided and/or third-party APIs, Web services, and similar technology.
Tech.05	to support "Punch-out Catalogues" – Leveraging a 3rd party, external catalogue to shop and pull information back into the e-procurement system for completion of the order, using industry standard protocols that is non-proprietary.
Tech.06	to support Web pages and Web feeds encoded in UTF-8.
Tech.07	to support real time integration leveraging web services architecture such as REST (HTTP bound, JSON and/or XML encoding) and SOAP (HTTP and/or JMS bound).
Tech.08	to support application server "scalability and performance tuning" functionality, through both: - Scalability built-in: a. An integrated function; and b. an external capability. - Required performance tuning functionality includes, but is not limited to: a. Dynamic load balancing; b. Clustering; and, c. Caching of components of the application environment to increase performance.
Tech.09	to support N-Tier application architecture pattern. There must be clear separation of user interface, application logic and data. Components must be loosely coupled.
Tech.10	to provide distinct staging environment(s) as necessary for the purpose of configuring, testing and training for the new software releases.
Tech.11	to support the capability of versioning of configurations, and the ability to roll back to previous production versions.
Tech.12	to support the capability of producing full database export to a native database file format.
Tech.13	to support best practices for securing web services, such as NIST SP 800-95 Guide on Secure Web Services

SOW NUM	Requirement
	Or NIST SP 800-44 Version 2 Guidelines on Securing Public Web Servers.
Tech.14	to support automatically terminating an open web session after a period of inactivity, to be determined by GC.
Tech.15	to support any database to handle manage and protect data up to Protected B level.
Tech.16	to support the solution in a segregated network and a zoned environment such that the EPS infrastructure is divided into zones respective of trust level such that: a) logical separation of data is preserved; and b) physical separation is connected through boundary devices.
Tech.17	to support functionality to allow users to export outputs such as reports and search results, including information in tabular and graphical format, in the following file format. a. PDF (Adobe PDF) b. DOC, DOCX(MS word 2007 and above) c. XLS,XLSX (MS Excel 2007 and above)
Tech.18	to support the current GC Internet Browser standard – Microsoft Internet Explorer 11, and two previous major versions when the standard changes.
Tech.19	to support the compatibility with major internet browsers on the market – e.g. Firefox, Safari and Chrome.
Tech.20	to support the capability to run as a secure web browser-based solution that does not require any other desktop software to be installed on the User's workstation besides a web browser.
Tech.21	to support master data management capabilities that include publishing and subscription services, via ESB, for connected systems (e.g. DFMS and other systems introduced by FMT).
Tech.22	to support the capability of accepting and uploading solicitation documents and attachments of file size up to 50Mbytes and any formats (e.g. CAD drawings, maps, movies).
Tech.23	to support the capability where a user can navigate directly to an actionable screen from the notification requesting an action, without logging-in again.
Tech.24	to support validation and confirmation of data entry by field type, data sizes, table properties and pre-configured list of values (e.g. only valid postal code format will be accepted for postal code).
Tech.25	to support the architecture style that enables robust error handling, recovery and notification to users when online errors occur.
Tech.26	to support best practice web application design principles for usability, i.e. W3 Web Application Best Practices. For example, enabling/disabling buttons, options and flows based on user entered values, reducing needless prompting, etc.
Tech.27	to support the capability to detect and support users with lower bandwidth network e.g. By offering smaller sized picture files on product catalogs.

SOW NUM	Requirement
Tech.28	to support a single sign on within the solution domain.

4.7 SECURE ACCESS

4.7.1 Overview

The purpose of this section is to define the user authentication requirements for the EPS. In the context of EPS, secure access refers to the ability to permit or deny user access to resources within the EPS system.

Given the diverse user base of the EPS, GC users, Provincial Government users, system administrators (including Contractor operators), suppliers (including international suppliers) and the general public, the EPS will require Secure Access for 3 General Groups of users:

4.7.2 Group 1: GC users.

The EPS must interoperate with the GC's Identity, Credential and Access Solution (ICAS) service. Currently, GC has only defined the Credential Management component of this solution. The following components available with credential management are:

Managed user credentials;

Authentication service for protected and non-protected information; and,

Support of Digital Signatures

Credential management is supported by Shared Services Canada (SSC) and is referred to as the Internal Credential Management (ICM) service. The service is based on Public-Key Infrastructure (PKI) technology and is named 'myKEY'. 'myKEY' is currently in use by the majority of employees across GC for authentication purposes to various GC systems. Treasury Board Secretariat (TBS) is developing an Identity, Credential and Access Solution (ICAS) Strategy which will lead to a full service government-wide digital signature facility.

4.7.3 Group 2: Non-GC users.

There is a corresponding external credential that is available to Non-GC users which is called "GCKey". GCKey is a Government of Canada-Branded secure credential service supported by Shared Services Canada. It is expected that GCKey, or equivalent, will be used for secure access to EPS by all non-GC users (i.e. Provincial government users, suppliers (including international suppliers and the general public when required).

4.7.4 Group 3: Contractor Resources.

The Contractor awarded the Contract to deliver, enable and support EPS is also required to provide an identity, credential and access management service for all Contractor resources providing support

for the EPS (such as, but not limited to, Service Infrastructure Operators, System Administrators, Service Operator accounts).

Please refer to the Security Annex 2 for detailed requirements for Identification and Authentication Management and Access Control.

References:

Guideline on Identifying Authentication Requirements: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262 (Treasury Board Secretariat).

ITSB-111 (July 2015): Cryptographic Algorithms for Protected Information https://www.cse-cst.gc.ca/en/node/1428/html/25015(Communications Security Establishment). (Supersedes ITSA-11A).

ITSG-31: https://www.cse-cst.gc.ca/en/node/267/html/22784 (Communications Security Establishment).

https://clegc-gckey.gc.ca/j/eng/AB-01

Table 92 -Secure Access Requirements for GC Users

SOW NUM	Requirement
SecureInt.00	**Internal** **Users** The Contractor must deliver a solution that provides the functionality:
SecureInt.01	to accept and authenticate Government of Canada managed user credentials for secure access to the solution using the GC's Identity, Credential and Access Solution (ICAS) (currently known as myKEY).
SecureInt.02	to support interoperability with the myKEY authentication service.
SecureInt.03	to be compatible with and use SAML 2.0 and OPENID Connect 1.0.
SecureInt.04	to be compliant with and interoperate with myKEY (PKI-based) authentication methodology to enable secure identification and authentication of GC users.
SecureInt.05	to be compliant with the Lightweight Directory Access Protocol (LDAP).
SecureInt.06	to ensure no simultaneous logons are allowed into the EPS for the same unique user account.

Table 93 - Secure Access for External Users (non-Government of Canada)

SOW NUM	Requirement
SecureExt.00	**External** **Users** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
SecureExt.01	to integrate with the GC's GCKey for external resources (non-GC).
SecureExt.02	to provide a self-registration interface. The interface must allow for delegation of authority within a corporation / company (to allow multiple users within a company/corporation).
SecureExt.03	to link a GCKey credential to an EPS user account.
SecureExt.04	to authenticate a user using GCKey at logon to the EPS.

PART 5: FUNCTIONAL REQUIREMENTS

5.1 INTRODUCTION TO THE FUNCTIONAL REQUIREMENTS

The functional requirements specify the scope of work including specific activities to be performed by the Contractor, as well as overall capabilities the solution must include while adhering to applicable legislative and policy mandated requirements specific to each sub-activity.

Principles:

The purpose of the functions described in this section is to ensure that the EPS will support the following principles:

- The EPS must be an easy to use and a flexible tool that can be readily configured by GC users and suppliers to reflect their specific requirements.
- Access to the EPS and its functionality will be based on defined user roles and responsibilities.
- The EPS will have workflow and business rules (including audit and compliance capabilities) to be configured by GC authorized users to support a wide variety of processes, activities and functions (as further described below).
- The EPS will assist the GC in continuing to reduce the administrative and paper-burden in the procurement process; while maintaining avenues to support manual (fax/ by mail / in person) processes where needed.
- The EPS will allow for the effective management of data – i.e. any and all data will be entered once and validated within the solution, with the ability to re-use and leverage data throughout the solution and across its functionalities from CLM to catalogue activities.
- The EPS will allow for seamless data sharing within the solution and to / from other related systems hosted by GC (e.g. SAP, etc.) to support the re-use of commonly required data in a secure manner across GC systems and for multiple purposes.
- The EPS will allow for dynamic and real-time (or close to real time) access to data, reporting and analytic information to support establishment and implementation of appropriate procurement strategies, monitoring and tracking of procurement processes and performance, and management and business decision-making.
- The EPS will allow suppliers to create and manage user accounts to access EPS.

5.2 FUNCTIONAL REQUIREMENTS LAYOUT

Each section of the functional requirements includes an overview, detailing the high level outcomes and process objectives of the mandatory requirements. The sections include:

5.2.1 Section A: General Functional Requirements

The general requirements for the EPS identify cross-cutting, high level functions and outcomes that are applicable across all elements of the EPS and all phases and activity streams.

The section includes requirements to maximize flexibility in configuring manual and automatic workflow processes for various types of user roles throughout the entire EPS, while ensuring that it

can handle multiple complex workflows, including inter-organizational and organization with different Delegation of Authorities and approval processes.

5.2.2 Section B to J – Functional Requirements

The overall functional requirements structure is a top-down approach detailing the phases and processes in the procurement environment. The required outcomes for these activities are purposefully generalized to allow Bidders the flexibility to develop a solution that meets the overall objectives of the procurement including enhanced electronic activities, streamlined administration, and improved client service including self-service tools.

The functional requirement sections are:

- SECTION B: PORTAL
- SECTION C: SOURCING AND CONTRACT MANAGEMENT
- SECTION D: PROCUREMENT MANAGEMENT
- SECTION E: SERVICE PROCUREMENT MANAGEMENT
- SECTION F: FINANCIAL MANAGEMENT
- SECTION G: BUSINESS INTELLIGENCE
- SECTION H: SUPPLIER RELATIONSHIP MANAGEMENT
- SECTION I: DATA AND INFORMATION MANAGEMENT
- SECTION J: USER MANAGEMENT

5.3 SECTION A – GENERAL REQUIREMENTS

The general requirements for the EPS identify cross-cutting, high level functions and outcomes that are applicable across all elements of the EPS and all phases and activity streams.

Table 94 - General Requirements

SOW NUM	Requirement
A-01.00	**GC Web Standards** The Contractor must deliver a solution that provides the functionality:
A-01.01	to deliver a service that meets the Government of Canada's Web Standards established by the Treasury Board (http://www.tbs-sct.gc.ca/ws-nw/index-eng.asp), that include the Standard of Web Accessibility, the Standard on Web Usability, the Standard on Web Interoperability, and the Standard on Optimizing Websites and Applications for Mobile Devices.
A-02.00	**Search** The Contractor must deliver a solution that provides the functionality:
A-02.01	to: • search for all documents, procurements and associated procurement data such as solicitations (RFx), contracts, requisitions, approval documents, clauses in a clause library, suppliers, scorecards, surveys, tasks, projects, etc.; • search based on reportable fields, document attributes and metadata;

SOW NUM	Requirement
	• search using wild cards, date ranges; • save contract searches for quick reuse; • have a system admin role publish a search to be used by end users; • to export results of search (e.g. CSV, text file); • sort and filter search results by criteria (such as, supplier, commodity code, item etc.); • perform a federated search of all catalog content (including punch-out catalogues); • to process full text indexing so that all text within the solution is searchable; and • to provide semantic suggestions based on the user's search keywords.
A-03.00	**Usability & User Interface** The Contractor must deliver a solution that provides the functionality:
A-03.01	that: • provides an intuitive, user-centric interface for suppliers, end-users and specialists, by leveraging the latest in Web and user design technologies and a focus on a minimal number of clicks; • incorporates best practice web application usability tools and plug-ins, such as mouse-over details, auto-complete/suggest, calendar scheduler, multi-select combo box, date picker, drag and drop manager, hot-keys, etc. • allows a user to navigate directly to an actionable screen from the notification requesting an action, or allow for direct approval within the e-mail; • allows draft transactions (e.g. contract, template, clause, sourcing event, evaluation, etc.) to be saved as in-progress work and be revisited at a future point in time; • enables auto save documents / forms at frequent intervals so that users having network problems can quickly pick up their work on a particular transaction; • should not require the user to add attachments more than once but rather reference the already uploaded attachment in situations where an attachment may be referenced in multiple locations (e.g. a contract and a sourcing event); • enables the configuration and application of default values for common data entry fields (i.e. financial coding, delivery address, invoice address, etc.); and • enables the addition of user-defined fields to any screen in various transactions.
A-04.00	**Online Help** The Contractor must deliver a solution that provides the functionality:
A-04.01	to: • provide a configurable Reference section that contains links to quick reference guides, manuals and policies; • provide in-application help and user support for functionality and processes; • provide the User with wizard-type steps and guidance on how to complete particular task or activity (e.g. how to write a SOW, submit a Bid, Supplier's Manual, etc.); • provide configurable 'hover-over' tooltips help functionality; and

SOW NUM	Requirement
	• enable presentation of context sensitive help topics aligned with the section of the tool the user is currently on.
A-05.00	**Error Messages & Notifications** The Contractor must deliver a solution that provides the functionality:
A-05.01	to: • allow authorized administrators to configure and control system notifications and notification triggers; and • provide system error messages and notifications in clear, concise, non-technical terms that can be understood by a non-technical User.
A-06.00	**Documentation** The Contractor must deliver a solution that provides the functionality:
A-06.01	to: • provide the Government of Canada (GC) all documentation and collateral material that is available for its current commercial offering and all future releases; • ensure that common terminology is consistently used throughout the EPS documentation, with input from the Project Authority on relevant Government of Canada (GC) terms; • allot sufficient time for documentation or process review and approval by the Project Authority based on mutually agreed to plans; and • provide electronic deliverables in a format that is approved by the Project Authority.
A-07.00	**Electronic Authorizations and Secure Electronic Signatures** The Contractor must deliver a solution that provides the functionality:
A-07.01	Electronic Authorizations and Secure Electronic to use electronic authorizations and secure electronic signatures for all authorizations within EPS. Electronic Authorizations and Secure Electronic Signatures must be implemented in a manner consistent with the Secure Electronic Signature Regulations and the Directive on Electronic Authentication and Authorization of Financial Transactions, and must ensure that: • access to electronic systems that store or process financial or finance-related transactions is restricted to those who require it to perform their duties; • user authentication information, such as identifiers and passwords, are properly safeguarded and managed, and users understand their accountabilities; • the identity of the authorizer is authenticated, and the proof of authorization is linked to every transaction that was authorized, at the time of authorization; • the authorized individuals approving transactions, including those exercising account verification, monitor the accuracy and appropriateness of the transactions and are informed of their accountabilities; • the authorization is consistent with the approved departmental delegation of authorities matrices in place at the time of authorization and appropriate separation of duties; and • an audit trail is maintained and records retention and disposition are managed in

SOW NUM	Requirement
	accordance with appropriate legislation, regulations and policy instruments so that the sequence of events and the transactions processed can be reconstructed for the purposes of an audit, investigation or review.
A-08.00	**System Configuration** The Contractor must deliver a solution that provides the functionality:
A-08.01	for the authorized administrator to create and configure web based forms with any number of configurable fields including, but not limited to: a. evaluation tables b. supplier response forms c. templates and documents d. surveys e. user defined fields
A-08.02	for authorized administrators to: • set fields as mandatory or optional; • configure and set default values for common data entry fields; • add user-defined fields to any screen in various transactions; • administer existing and define new data elements with various characteristics such as predefined validation rules, value ranges, dropdown lists, free form texts with user defined length maximums; • configure and create different types of extrinsic fields (e.g. text, radio groups, checkboxes, drop-down lists, money, date, etc.); and • to modify out of the box field labels.
A-08.03	to automatically notify users of incomplete mandatory data fields.
A-09.00	**Guided Navigation** The Contractor must deliver a solution that provides the functionality:
A-09.01	to provide Buyers with a guided or wizard-type process to assist Buyers in navigating to the right procurement methodology for the goods or services.

5.3.1 Workflow

The overall objective of this section of requirements is to maximize flexibility in configuring manual and automatic workflow processes for various types of user roles throughout the entire EPS, while ensuring that it can handle multiple complex workflows, including inter-organizational and organization with different Delegation of Authorities and approval processes.

Table 95 - General Requirements – Workflow

SOW NUM	Requirement
A-10.00	**Workflow - General** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
A-10.01	for an authorized administrator to configure and manage role-based workflow instances that support manual and automated process steps (system and user-defined fields) in each functional area (e.g. procurement review & approval, supplier/user registration, records/document management, payment method).
A-10.02	for an authorized administrator to configure and capture approvals using sequential, parallel, hierarchical, and inter-organizational workflows.
A-10.03	for an authorized administrators to configure a workflow template and to allow authorized administrators to configure exceptions (e.g. additional workflow steps, overriding a mandatory workflow step, etc.).
A-10.04	for authorized administrators to add additional workflow steps that are applied only to that specific workflow instance and not to the workflow template itself (e.g. adding ad-hoc approvers).
A-10.05	for an authorized administrator to configure a workflow such that authorized administrators can complete multiple sequential approvals under a single operation (e.g. batch of approvals).
A-10.06	to configure the default step the workflow returns to when a rejection occurs.
A-10.07	for users to provide a reason and comments when rejecting/approving/escalating a request.
A-10.08	for users to stop, pause, resume, and recall a workflow at every step.
A-10.09	for authorized administrators to view the status of the workflow progress.
A-10.10	for users to configure automatic and manual workflow escalation procedures (e.g. time period).
A-10.11	for users to reassign the workflow task to another user with the same role.
A-10.12	for authorized administrators, within a group, to assign a workflow step to a single member assigned to that group.
A-10.13	to automatically assign a workflow step to an administrator and notify the originator in the event that the step identified a group or role no longer available (e.g. no users in a group, group renamed).
A-10.14	for a user, within a group, to indicate a workflow step will be actioned by that user and no other group member.
A-10.15	to enable the use of a graphical or textual tool for creating and configuring workflows and testing them in a simulated environment.
A-10.16	to provide error information to users during the creation of the workflow (e.g. error messages for logic errors in workflow creation) and to provide information to the users as to why a workflow cannot proceed.
A-10.17	to support built-in tutorials to facilitate the configuration of a workflow by authorized administrators.

5.3.2 Workload

Workload will provide GC users with the ability to assign files and activities to GC resources, to monitor and measure performance against assigned tasks, as well as to effectively allocate and re-allocate workload across multiple resources, resource groups and organizations.

Table 96 - General Requirements – Workload

SOW NUM	Requirement
A-11.00	**Workload - Assignment** The Contractor must deliver a solution that provides the functionality:
A-11.01	for the authorized administrator to configure and manage up-to-date lists of procurement team resources (e.g. by division, category and commodity taxonomy).
A-11.02	for the authorized administrator to configure business rules and formulas for automatic and manual assignment and re-assignment of procurement file to members of the procurement team.
A-11.03	for the authorized administrator to manage team members participating in the sourcing event, including, but not limited to: a. assign a backup team member to a file, task and activity for the specified time period; and b. revert all related files, tasks and activities back to the originally assigned team member when acting ends.
A-11.04	for the authorized administrator to manage team members participating in the sourcing event, including, but not limited to: a. add and remove team members; b. assign team members permissions and roles; and c. assign files, tasks and activities to team members.
A-11.05	for the authorized administrator to assign durations to each assigned task, activity, milestone in a project so that procurement team member workload can be determined.
A-11.06	for the authorized administrator to configure automatic escalation routines in the event a procurement file sits in queue beyond certain thresholds (i.e. time based).
A-11.07	for the authorized administrator to set business rules to assign a new procurement file automatically to a specific team or individual resource based on combination of parameters including but not limited to: a. designated commodity classification; b. dollar value; c. client geographical location; d. availability; e. working unit; and f. role of the procurement team member.
A-11.08	for the authorized administrator to review procurement file information and manually re-allocate the procurement file to another group, division or individual.

SOW NUM	Requirement
A-11.09	to quantify and determine existing workload for each team member based on configured and applied formulas and calculations.
A-11.10	for the authorized administrator to configure priority designations for assigning and re-assigning priority to the procurement files and documents based on criteria such as, but not limited to: a. urgency; b. required delivery date; and c. management instruction.
A-12.00	**Workload - Tracking and Status** The Contractor must deliver a solution that provides the functionality:
A-12.01	for authorized administrators to configure display formats, business rules and set indicators and alarm triggers for tracking the status of individual and team workloads (e.g. based on the commodity).
A-12.02	for authorized administrator to accurately track and record performance metrics on any procurement file.
A-12.03	to display individual and team procurement workload information in various formats including, but not limited to, tabular, graphs, charts.
A-12.04	to display workload indicators and trigger alarms based on the procurement file activities and individual or group workloads.
A-12.05	for users, according to their permissions, to view and track workload information such as, but not limited to: a. team and individual workloads across each department, region, client; b. workload and allocation of the procurement files and documents for each team member; and c. scheduled activities, tasks, milestones for each individual user.
A-12.06	for authorized administrators to view all key workload information related to the procurement files in one workspace including but not limited to: a. stage and status of their files; b. status of related documents; c. status of related activities; d. snapshot of their workload; e. location of each workload item; and f. relevant workload dates.
A-12.07	to facilitate access to the most recently saved procurement file and all related documents and allow authorized administrators to track and link requisition with all components of procurement file.
A-12.08	for users to sort, filter and aggregate workload items.
A-12.09	for authorized administrators to track procurement pipeline and provide insight into planned procurement activities and when they need to be executed.

5.4 SECTION B – PORTAL REQUIREMENTS

5.4.1 Objective

The objective of this section is to describe the requirements of the Portal within the overall scope of the EPS to ensure that the proposed portal component of the service is robust and comprehensive.

The GC's high-level business objectives as they relate to the requirements of portal are:

- to deliver a comprehensive interface to all users (internal and external) to the solution and associated services, information, training and support;
- to present all users with at-a-glance information that is most relevant to their roles and responsibilities;
- to enable one-time login for users and have authenticated access to all components of the solution;
- to establish a secure, reliable and accessible "one stop shopping/one stop selling" experience for all users; and

5.4.2 Complexity

The proposed solution must be able to handle and respond to the complex environment of the GC. Some elements that contribute to the complexity of the organization are:

- The GC is a large, complex organization (over 250,000 employees).
- Users will come from various departments, each with multiple levels of hierarchy.
- Users will have varying delegations on a specific and general basis.

5.4.3 Key Deliverables

The portal must provide access to the functionalities specified below and outlined within the various sections of the Statement of Work.

Content and Data: allow users to create, edit, review, approve and publish content in the portal.

Landing Page: allow for the creation and configuration of specific page(s) on a web site for the general public such as:

- registration to generate a user profile;
- deliver relevant communications; and
- provide information on what is available through the service

Dashboards: within the dashboard, enable the following functionalities:

- set goals and expectations for specific individuals or groups;
- encourage specific actions in a timely manner;
- highlight exceptions and provide alerts when problems occur;
- communicate progress and success; and
- provide a common interface for interacting with and analyzing important business data

Communication: enable and facilitate the delivery of key messages within the portal.

5.4.4 Government Electronic Tendering Services (GETS)

The Contractor must provide the functionality to: deliver, enable and support a tendering portal as described in this section.

5.4.4.1 Introduction / Background:

The GC has an ongoing need for electronic tendering services to meet international trade obligations for open competitive procurements. These services, known as Canada's Government Electronic Tendering Service (GETS) are expected to be provided under the new EPS.

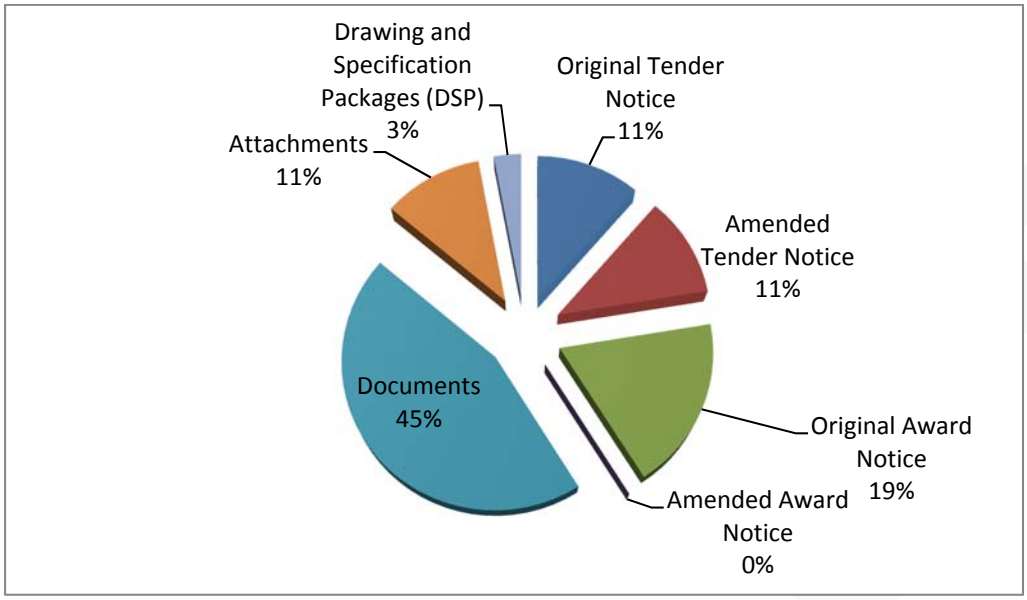
Procurement policies require Canada to use open competitive procurement processes including utilizing electronic tendering services to acquire goods and services. The GC has been utilizing a custom developed tendering system known as BuyandSell.gc.ca/tenders since 2013. EPS is intended to replace the BuyandSell.gc.ca/tenders GETS platform.

Public Tender Volumetric:

Over a 12 months period (May 2014 – April 2015):

- 3,415 GC tenders averaging 13.8 tenders per working day were published on BuyandSell.gc.ca/tenders and of that, 1,478 tenders averaging 5.9 tenders per day were published by PWGSC; and
- 60,931 tender documents including Original Tender Notices, Amended Tender Notices, Original Award Notices, Amended Award Notices, Documents, Attachments, Drawing and Specifications Packages were uploaded on BuyandSell.gc.ca/tenders. The file sizes ranged from a few hundred bytes to gigabytes mainly for Drawing and Specification Packages (DSP). (Figure 7)

Figure 6 - Buyandsell.gc.ca – Metrics



5.4.4.2 Functional Deliverables

In support of the Government Electronic Tendering Service, The Contractor must provide the functionality to: deliver/enable the following:

Tender Notices on the Government Electronic Tendering Service (GETS)

For procurements subject to trade agreements, a tender notice that a solicitation opportunity is available must be posted on GETS specifically when using open tendering and selective tendering processes.

To meet the requirements of the Comprehensive Economic Trade Agreement (CETA) with the European Union, GC must provide a single site on which all public sector tenders must be published. This capability will be required within 5 years of the ratification. Ratification of the CETA is targeted for late-2016. The EPS will provide this functionality, and support all federal electronic tendering as well as posting for all other public sector tenders.

All tender notices must be prepared and posted in both official languages.

As the Single Point of Access for government tenders, GETS must deliver, enable and support multiple sources and methods for creating tender notices, including:

- The creation and publication of tender notices including attachments to GETS through EPS as part of an e-sourcing activity.
- The manual creation and publication of tender notices including attachments to GETS for users not leveraging EPS for sourcing activities.
- The aggregation, publication, and updating of tender notices including attachments from third party systems and data feeds.
- The configuration of publishing cycle times for batch or individual transmission of tender notices.

- Automatic update of active tender notice (including attachments) on GETS in support of any revisions initiated and approved through EPS (e.g. amendments, cancellation, and termination).
- Manually change or cancel in real time, tender notices that are in queue to be published (tender notices that have not yet become active on GETS).
- Automatic application and control of tender notice status and version (e.g. Active, Amended #, Expired, Cancelled, and Awarded).
- Automatic archiving of expired procurement opportunities so they are separate from open bid opportunities.

5.4.4.3 Award Notices

For procurements subject to trade agreements, an award notice must be posted on GETS within 72 days of contract award (configurable publishing cycle time). Although there are no minimum time periods identified for the Agreement on Internal Trade (AIT), the 72-day limit applies for reasons of consistency.

For all contractual documents issued through the EPS, award notices must be generated automatically through EPS, except when a "National Security" consideration has been identified. For procurements subject to the trade agreements where EPS is not used for contract award, contracting officers must have the ability to manually create and post award notices.

5.4.4.4 Services Supporting Supplier's Access to Opportunities

The ability for suppliers to easily find and access government opportunities is paramount. GETS must ensure Suppliers:

- can easily find opportunities relevant to their business; and
- get the most up-to-date information about tender notices and amendments;

The Contractor must provide functionality for a GETS to support these objectives:

- Electronic Subscription Services**:** registered suppliers must have the option to subscribe to receive email notifications of new bid opportunities based on the region, organization, and/or type of product/service (commodity code) and to amendments or modifications of tenders that the supplier had indicated an interest in.

- Create a web feed to follow a solicitation: registered suppliers must have the option to subscribe and receive web feeds for specific bid opportunities they intend on responding to in EPS.

- Bookmark Search Results: registered and unregistered users must be able to search published tender notices, save, bookmark and share the URL (the Webpage address). The URL is must stay the same when new information becomes available.

- Organize, filter and Sort: registered and unregistered users must be able to:

- Filter the way they want to list and display all open bid opportunities on GETS.

- Access tender notices by goods and services categories (i.e. Goods, Services, Services related to Goods, Construction) and/or browse by status (e.g. New today, Amended Today, Active, Closing in 24 Hours, Expired, Awards).

5.4.4.5 Services Supporting Supplier's Ability to Analyse Opportunities and Forge Partnership

The ability for suppliers to analyse published opportunities and forge partnerships for the purpose of increasing their chances of success and providing quality bids is paramount.

The Contractor must provide functionality for a GETS to support these objectives:

- **List of Interested Suppliers (Bidder Request List):** GETS must capture and make publically available as part of the tender notice, a list of suppliers that have registered their intent to submit a response to a bid solicitation in EPS. This list is not required to be made available as part of the open tender data file.

- **Analyze Procurement Data:** all procurement data on GETS must be provided in open data format for easy download by any user.

- **Access Anonymous Web Usage Statistics:** allow suppliers to access anonymous web usage statistics for each tender notice such as number of page views and notice documents downloads.

- **Share with one link:** allow suppliers to email or post a tender notice hyperlink (URL) to their social media accounts to express their interest in collaborating on a specific bid opportunity. The tender information must always be current to indicate any revisions and amendments.

- **Use or establish third-party services:** the private sector including tender publishing companies, industry associations and others must be able to subscribe to syndication feeds.

5.4.4.6 Open Tender Data

GC is committed to open data and advancing the Government of Canada's Action Plan on Open Government and the Red Tape Reduction Plan by empowering citizens to participate in government through information sharing. The GC is committed to ensuring data on government opportunities is freely available.

GETS must be an open service and can be accessed anonymously without the need to register and with the right to distribute or republish tender data on another Web site. All GETS tender data must be made available as open data in accordance with Part 2 Legislation, Regulatory and Policy Requirements and Section "I", Data and Information Management. The Contractor must not restrict the ability for third parties to re-publish tender information.

5.4.5 Portal Requirements

Table 97 - Portal Requirements

SOW NUM	Requirement
B-01.00	**General** The Contractor must deliver a solution that provides the functionality:
B-01.01	for authorized administrators to electronically and in near real-time create, edit, view, approve and publish content in the portal.
B-01.02	for users to view current and expired system notices in the Portal.
B-01.03	to allow authorized administrators to configure whether a data field (label and value) is visible or hidden on publicly available documents (e.g. Web pages, attachments) generated by EPS.
B-02.00	**Landing Page** The Contractor must deliver a solution that provides the functionality:
B-02.01	to configure and enable one-time login to provide role-based access to all components of EPS.
B-02.02	for authorized administrators to configure and manage help section (e.g. introduction to the Portal, its features, user/supplier login, supplier registration user guide, and Frequently Asked Questions, knowledge-based online training).
B-02.03	to configure the Terms of Use of EPS in order that it appears at various predefined stages of the process to confirm acceptance of the EPS (configurable reoccurrence).
B-03.00	**Dashboard** The Contractor must deliver a solution that provides the functionality:
B-03.01	for authorized administrators to configure and utilize various reusable templates with different features and controls including the ability to select from a variety of configurable dashboards.
B-03.02	for authorized administrators to create multiple dashboard templates within one workspace.
B-03.03	to automatically control dashboard content based on user role and pre-established business rules.
B-03.04	for users to configure various default parameters within their dashboard (e.g. filter dates, visual appearances, font size & colour, turn on or off non-mandatory alerts).
B-03.05	for users to upload and download documents of all file types.
B-03.06	for users to organize their dashboard including reports, links to other applications and web based content.
B-03.07	for users to utilise hierarchical operations when displaying data at multiple levels of aggregations such as ``drill-down'' and ``roll-up'' operations.
B-03.08	for users to see two or more subsets of the data side-by-side.
B-03.09	for users to identify things in the dashboard that are important to them (starring/tagging).
B-03.10	for users to add commentary to specific numbers or charts (Annotation).

SOW NUM	Requirement
B-03.11	to automatically generated textual description of the key information in the dashboard.
B-03.12	to support and utilize a variety of visualization models (e.g. charts and graphs).
B-03.13	to display performance and business information snapshots to users based on their role.
B-03.14	to display a user's actions (to dos) and notifications.
B-03.15	for users to view, search and organize (e.g. sort and filter) the status and associated timelines for each of their work activities (e.g. sourcing activities, shopping cart request order tracking, order confirmation, open requests for quotation, and all confirmed orders).
B-04.00	**Communication** The Contractor must deliver a solution that provides the functionality:
B-04.01	to enable and facilitate the communication between Suppliers and Buyers in the catalogue environment (e.g. sending an e-mail within EPS, etc.).
B-04.02	for users to access message history for all communications between buyers and suppliers specific to each procurement file.
B-04.03	to configure notification message and distribute as per established workflow steps (e.g. approval requests, Status of invoice/good receipt, credit memo).
B-04.04	to notify authorized administrators when Supplier has: - acknowledged their requests (e.g. request for quote), Orders and messages within EPS; - not acknowledged their messages by a configurable time period within EPS.
B-04.05	for authorized administrators to create and distribute electronic, outward communication to portal users.
B-04.06	to create and communicate to all portal users or a user generated subset of portal users (e.g. at a minimum, being able to create e-mail distribution lists).
B-04.07	to alert authorized administrators in near real-time, via email notifications, if errors (e.g. HTTP errors) are raised during the operation of EPS.
B-04.08	to provide on-screen alerts with highlighted information and allow user to close them only by acknowledging the content (e.g. notification of system maintenance).
B-05.00	**Government Electronic Tendering Service (GETS)** The Contractor must deliver a solution that provides the functionality:
B-05.01	for authorized administrators to configure publishing cycle times for batch or individual transmission of tender notices to Government Electronic Tendering Service (GETS) site.
B-05.02	for users to change or cancel in "real time", tender notices that are in queue to be published (tender notices that have not yet become active on GETS) or tenders that have been made public.
B-05.03	to automatically push specific content including attachments from EPS to Government Electronic Tendering Service (GETS) site, accessible to all users including unregistered users.

SOW NUM	Requirement
B-05.04	for the manual creation and publication of different tender notices including attachments to Government Electronic Tendering Service (GETS) for users not leveraging EPS for sourcing activities.
B-05.05	to automatically update active tender notices (including attachments) on Government Electronics Tendering Service (GETS) site in support of any revisions initiated and approved through EPS (e.g. amendments, cancellation, termination).
B-05.06	to automatically apply and control the status and version of the tender notice (e.g. Active, Amended #, Expired, Cancelled, and Awarded).
B-05.07	to automatically archive expired tender notices so they are separate from open bid opportunities.
B-05.08	to transmit notices to other web portals, email addresses through subscription (registered users and unregistered users).

5.5 SECTION C: SOURCING AND CONTRACT MANAGEMENT

5.5.1 Creating a sourcing event

The objective within the sourcing event creation environment is to provide a Consumer-Like experience to a casual user (non-procurement expert), which will guide the user through the requisition creation process, and provide online collaboration between the contracting authority and the casual user during all phases of a sourcing event.

Where an item is not located within an existing e-Catalogue, the user will be required to submit a Requisition to initiate a Sourcing Event. The Requisition will trigger the development of the procurement plan and strategy, where decisions will be made that will contribute to the development of an RFx that will be used to solicit offers/proposals from one (1) or more suppliers.

GC users with administrative rights will establish templates for RFx, which will provide for configurable and customizable electronic documents that will then be populated by other GC users based on the confirmed Procurement Strategy and Plan and the specifics of the GC user's requirements for goods and/or services. The GC user will create a Catalogue Data File, within the RFx, based on the nature of the procurement requirement (e.g. commodity, dollar value, etc.) and populate the Catalogue Data File with the goods and services that suppliers will be required to bid on during the Sourcing Event. (It is important that the applicable information persists from the Sourcing Event to the e-Catalogue area without requiring the information to be extracted from the system, manipulated and then imported to the e-Catalogue). The resulting RFx document (which includes the catalogue data file) may be distributed directly to one (1) or more supplier(s) or may be publicly posted for access by any potential supplier(s).

The e-Sourcing functionality will provide a means for communications and collaboration between Suppliers and the GC user (e.g. allowing for development and distribution/publication of Questions and Answers, Addenda to the RFx, etc.) and will provide a secure means of Supplier bid creation and/or submission (for electronic proposals) or recording of bid receipt (for hard-copy proposals).

The RFx may include structured form-fillable and configurable templates for use by Suppliers in responding to the RFx such as Statement of Work (SOW) and Evaluation Criteria – to support Suppliers in responding directly to the specific requirements of the procurement as well as to facilitate evaluation of submitted offers/proposals by the GC against each identified Evaluation Criterion. The e-Sourcing functionality must also support this evaluation process through providing a secure and structured environment wherein the contracting authority may collaborate with other GC users authorized to view, evaluate and comment on the Suppliers offers/proposals to identify the successful qualified Supplier(s) in accordance with the Criteria and process set out in the applicable RFx.

The EPS must support the notification of Suppliers of the results of the RFx process, and must allow GC users to create the contract/framework agreement and award; including the necessary reviews and approvals.

In some cases, when creating a Sourcing Event, the GC user will configure the request for Supplier input to enable the information received to be persisted through the evaluation process and, if the Supplier is qualified, into the associated e-Catalogue; and across the EPS as appropriate.

Following Contract Award, the EPS must allow for tracking by GC users of delivery of the goods and services by suppliers, as well as for recording of performance, and evaluation by GC users of the performance of suppliers (e.g. on time, on budget, right quality, etc.). The EPS must also support GC users in conducting various Contract Lifecycle Management (CLM) activities, including but not limited to: creating and collaborating with Suppliers to implement amendments to the terms and conditions of the contract/agreement, extension of term, variation (up or down) in the quantity of goods/services ordered by the user, etc. and must also support the close-out of a contract/Framework Agreement (e.g. following final delivery by suppliers or in the event of another form of contract termination by authorized GC users) where appropriate.

The EPS must provide full integration of all its modules (workload management, sourcing management, supplier's relationship management, catalogue management) and be fully configurable to effectively manage sourcing events and contracts in compliance with all government objectives, policies, rules and regulations.

The e-Sourcing tool will be used to conduct one-off / complex procurement processes; to establish new or refresh existing Framework Agreements/Methods of Supply, create/maintain e-Catalogues and for ordering e-Catalogue items where a second-stage procurement process is required. The e-Sourcing functionality supports the requirements of the Sourcing and Contract Lifecycle Business Area.

This Business area is divided into the following sections:

C-01 Requisition Management - the EPS must enable a user to create, edit, save and electronically submit requisitions to authorize a Contracting Authority to:

- initiate a new sourcing event on their behalf to procure the required goods and/or services; and

- to initiate a contract amendment activity (i.e. exercising optional periods, increasing the level of effort, etc).

C-02 Planning and Strategy Development - the EPS must enable a contracting authority to configure, manage, and have access to required information to develop an effective procurement strategy.

C-03 RFx Creation - the EPS must enable an Authorized User to create a new or complete a user-selected RFx template (e.g. RFP, RFT, RFSO, RFSA, RFQ, etc) from drafting to final state for publishing.

C-04 RFx Posting - the EPS must enable an authorized user to publish the final RFx including all supporting documents through different means such as direct posting to a portal or other government websites, distribution via email, fax, etc.

C-05 Bid Submission - the EPS must enable registered suppliers to securely submit electronic bids and manual bids.

C-06 Evaluation - the EPS must provide the functionalities to enable authorized users to evaluate registered supplier responses and to make effective award decisions.

C-07 Contract Award - the EPS must enable authorized users to rapidly finalise and award contracts.

C-08 Contract Administration - the EPS must enable authorized users to track, monitor and support the management of the relationship between the department and the supplier from contract award to contract closeout ensuring the supplier delivers the product and/or service in conformance with the contract requirements.

C-09 Project Management – the EPS must enable users to apply Project Management best practices to create and manage procurement files by linking together all documents related to a sourcing event.

C-10 Central Repository – the EPS must enable authorized users to create and manage a clause repository (library) providing corporate and custom clauses in both official languages that can be accessed by a Contracting Officer to create RFx, RFx amendments, contracts, and contract amendments.

5.5.2 Requirements

Table 98 - Sourcing and Contract Management Requirement

SOW NUM	Requirement
C-01.00	**Requisition Management** The Contractor must deliver a solution that provides the functionality:
C-01.01	for authorized administrators to create and configure an intelligent requisition form governed by business rules that must prompt users for further information and documents based on information provided (e.g. Will ask for a copy of a Statement of Work if the user indicated the requisition is for a professional service).
C-01.02	for authorized administrators to create and configure various types of requisitions.

SOW NUM	Requirement
C-01.03	for authorized administrators to configure mandatory and optional fields in the requisition to control requisition data input.
C-01.04	for authorized administrators to configure the rules for assignment of unique identifier for each requisition to connect with Solicitation and Contractual documents.
C-01.05	for authorized administrators to configure routing, assignment and approval of electronically submitted requisitions and related documents.
C-01.06	to automatically manage and update requisition status through its lifecycle (e.g. Draft, Submitted for Approval, Amended, Rejected).
C-01.07	for the Requisitioner to configure their user profile to pre-populate repetitive data on the requisition (e.g. Requisitioner Name, Approver Name, Delivery Location, Billing Location).
C-01.08	for the Requisitioner to: a. create, view, save, retrieve, modify and amend Requisition with at least 1500 line items; and b. attach supporting documents to the Requisition.
C-01.09	to validate information entered by the Requisitioner against appropriate central repositories (e.g. UNSPSC Taxonomy).
C-01.10	for the Requisitioner to electronically certify availability of funds.
C-01.11	for the Requisitioner to assign multiple financial codes to a requisition.
C-01.12	for the Requisitioner to electronically submit approved requisition to the designated purchasing organization.
C-01.13	for the Contracting Officer and Requisitioner to collaborate at any time on the creation of requisition and supporting documents.
C-01.14	for the Contracting Officer to enter approved requisition, requisition amendments and attach related documents submitted outside of the system (e.g. Surrogate user function)
C-01.15	for the Contracting Officer to group and consolidate similar requirements based on a variety of parameters such as, but not limited to, commodity type, method of procurement, Delivery location, from different requisitions to facilitate group buying.
C-01.16	for the Contracting Officer to track each item from the requisition independently and provide traceability of the item back to the initial requisition.
C-02.00	**Planning and Strategy Development** The Contractor must deliver a solution that provides the functionality:
C-02.01	for the authorized administrators to create and configure and manage a variety of procurement templates that will assist Contracting Officer during planning and strategy development phase.
C-02.02	for the authorized administrators to configure and manage business rules and parameters in support of procurement risk and complexity assessment.

SOW NUM	Requirement
C-02.03	for the authorized administrators to configure and manage business rules and parameters to ensure compliance with corporate, national and international obligations.
C-02.04	for the authorized administrators to configure and manage access to various information sources that are external and internal to the solution including, but not limited to, relevant policies, rules and regulations (e.g. hyperlink to a policy that resides outside or inside of the solution).
C-02.05	for the Contracting Officer to access various internal and external information sources at any time during planning and strategy development.
C-02.06	to support iterative and continuous procurement assessment, approval, planning and strategy development during any time of procurement process before posting (e.g. if one does an amendment, assessment and approval process must restart).
C-03.00	**RFx Creation** The Contractor must deliver a solution that provides the functionality:
C-03.01	for the authorized administrators to configure triggers and alerts for other user's activities that have to be performed based on pre-established set of rules.
C-03.02	for the Contracting Officer to create and configure multi-phase Sourcing Events (e.g. LOI, RFI, RFP linked to single requisition).
C-03.03	for the Contracting Officer to create and manage RFx documents such as, but not limited to: a. Letter of Intent (LOI); b. Request for Information (RFI); c. Request for Quotation (RFQ); d. Request for Proposal (RFP); e. Invitation to Tender (ITT); and f. other RFx (RFSO, RFSA).
C-03.04	for multiple users to simultaneously work on and complete different sections of an RFx.
C-03.05	for the Contracting Officer to search central repositories for various artefacts and templates during RFx creation including, but not limited to: a. forms; b. RFx templates; c. contract templates; d. clauses and conditions; e. requirement; f. previously asked questions; and g. questions attached to supplier profile.
C-03.06	for the Contracting Officer to create new RFx documents and Model Contracts with user-defined configurable fields: a. without templates;

SOW NUM	Requirement
	b. from central repository of approved templates; and c. reusing all or parts of previously issued RFx.
C-03.07	for the Contracting Officer to search, identify and reference applicable Clauses and Conditions during RFx creation (e.g. hyperlink in the RFx template to the actual clause in the library).
C-03.08	for the Contracting Officer to select and insert pre-existing and define new bid evaluation criteria and scoring methodologies in the RFx document.
C-03.09	for the Contracting Officer to configure and apply selection methodologies such as, but not limited to: a. lowest priced responsive bid; b. the lowest responsive cost-per-point; c. highest responsive combined rating of technical merit and price; d. highest rated responsive bid within a stipulated maximum budget; e. lowest cost-per-point bid of only those bids that rank within a configurable percentage of the bid achieving the highest score for technical merit.
C-03.10	for the Contracting Officer to configure, test and apply simple and complex arithmetic and statistical formulas for technical and financial evaluation scoring.
C-03.11	for the Contracting Officer to configure and create financial response tables with embedded formulas to capture information such as, but not limited to, discounts, level of effort, quantity, tiered pricing.
C-03.12	for the Contracting Officer to select pre-existing and define new basis of payment for the solicitation.
C-03.13	for the Contracting Officer to configure rules in support of “sealed bidding” process.
C-03.14	for the Contracting Officer to preview layout and design of all configured forms(e.g. solicitation, evaluation matrix, pricing tables etc...).
C-03.15	for the Contracting Officer to select bid submission mode (i.e. Online, Offline, Combination of Online and Offline).
C-03.16	for the Contracting Officer to configure, define and use business rules, that will apply to resulting Contracts and Contract source lists (e.g. define logic for rotational, right of first refusal, refresh).
C-03.17	for the Contracting Officer to create multiple RFx against the same requisition.
C-04.00	**RFx Publishing** The Contractor must deliver a solution that provides the functionality:
C-04.01	to support various sourcing event’s models such as, but not limited to, open competitive, invitational competitive and directed procurement process.
C-04.02	for the Contracting Officer to create and manage reusable invitational source lists which includes, but is not limited to, Supplier names, Supplier profile, contact

SOW NUM	Requirement
	information, product/service listings, commodity codes and historical procurement award details for registered Suppliers.
C-04.03	for the Contracting Officer to search and manage source lists of suppliers using various search parameters including, but not limited to, commodity codes, key words, product/service, geographical location, security profile, availability.
C-04.04	to capture the required information provided by the Contracting Officer during RFx creation and pre-populate procurement notices for publication including, but not limited to, Solicitation Number, Region of Delivery, Solicitation Type, Taxonomies, Trade Agreements, Tendering Procedure, Publishing Date, Closing Date and Time.
C-04.05	for the Contracting Officer to manage bidding period and amend closing date for single or multiple sourcing events by configuring and enabling system generated duration based on the type of solicitation and/or National and International obligations and allow authorized administrators to override system recommendation.
C-04.06	for the Contracting Officer to publish open solicitations and distribute invitational solicitations for single and multi-phase Sourcing Events (e.g. LOI, RFI, RFP).
C-04.07	for the Contracting Officer to send electronic notification(s) to all or selected suppliers from a source list, informing them of the procurement opportunities, changes to the solicitation, etc.
C-04.08	for the Contracting Officer to send an electronic notification to the suppliers who downloaded the solicitation document each time when additional documents, amendments and notices are issued and published.
C-04.09	to support real-time and scheduled posting on Government Electronic Tendering Service (GETS) with option to delay, suppress or retract posting of sourcing events, notices and documents.
C-04.10	for the Contracting Officer to cancel an existing solicitation and publish cancellation notice to the Government Electronic Tendering Service (GETS).
C-04.11	for the Contracting Officer to amend the published version of RFx and related documents, highlighting amended sections and electronically notify suppliers of the revisions.
C-04.12	for the Contracting Officer to configure and extend qualification period for an RFx with On-Going opportunity (e.g. monthly, quarterly, semi-annually assessment).
C-04.13	for the Contracting Officer to configure a bidding clock in real time which supports time zones and automatically adjust for daylight savings time.
C-04.14	to display an event countdown clock to show the time remaining for sourcing event.
C-04.15	for suppliers to electronically submit questions to the designated Contracting Officer.
C-04.16	for the Contracting Officer to edit supplier questions and remove bidder specific information before: a. seeking a response from the designated authority; and

SOW NUM	Requirement
	b. sharing and/or publishing questions and answers with all participating suppliers at the same time.
C-04.17	for the Contracting Officer to manage and track all questions and answers while maintaining integrity of the original questions.
C-04.18	for authorized administrators to control whether bid opening is permitted during bidding period (e.g. before closing date for on-going opportunities).
C-04.19	for the Contracting Officer to view the RFx supplier activity log which at minimum indicates the number of suppliers who: a. viewed and downloaded an RFx; and b. viewed without downloading an RFx.
C-05.00	**Bid Submission** The Contractor must deliver a solution that provides the functionality:
C-05.01	for only registered supplier to complete and submit electronic bids and all related documents.
C-05.02	to guide supplier through the bid submission process (e.g. checklist or wizard).
C-05.03	to manage a multi-envelope electronic bidding process by allowing supplier to organize and submit their bids in multiple sealed envelopes (e.g. one technical, one financial and one certification).
C-05.04	to display a summary of supplier bid for a final review prior to submission.
C-05.05	to store and keep submitted bids in secured location until the designated bid closing time.
C-05.06	to disable electronic bid submission functionality at bid closing time.
C-05.07	to allow Contracting Officer to track all recorded information about received bids and bid submission activities including, but not limited to: a. bids received On-Line and Off-Line; b. exact date and time of each bid submission; c. when completed bids were retracted by the Supplier; d. when bids were re-submitted by the Supplier; e. list of files submitted with file names and file size; and f. when bids were accessed and by whom.
C-05.08	to generate an official record (e.g. electronic receipt) for both on-line and off-line bid submissions that includes details such as, but not limited to, Confirmation Number, Supplier ID, Supplier Name, Submission Name and Number, Date and Time received, Check List of Items Received, List of Items yet to be received.
C-05.09	to link bid attachments with related RFx sections and/or individual RFx requirements.
C-05.10	to enable supplier to import, edit and carry forward answers from previous sourcing events for the purpose of responding to repetitive requirements (e.g. ask once – tell once).

SOW NUM	Requirement
C-05.11	for the supplier to retract submitted documentation and/or completed bids and resubmit final bid prior to bid closing time.
C-05.12	for the supplier to provide reference information about posted bonds, security deposits or cheques with their bid submission.
C-05.13	for the supplier to submit bid pricing using downloadable spreadsheet applications (e.g. MS EXCEL).
C-05.14	to automatically check and validate completeness of the suppliers' responses.
C-05.15	to track status of the supplier bid submission stage (e.g. In Progress, Submitted, Retracted, etc.).
C-05.16	to check supplier's integrity and security against Supplier's Profile in Supplier Relationship Management (SRM) repository during and after bid submission and notify contracting officer of any status changes.
C-06.00	**Bid Evaluation** The Contractor must deliver a solution that provides the functionality:
C-06.01	to support a secure virtual evaluation environment through defined parameters and permissions set by authorized administrators through administration properties.
C-06.02	to keep bid evaluation information, such as, but not limited to, individual and consensus evaluation results in strict confidence and ensure that information is accessible only to authorized administrators.
C-06.03	for the Contracting Officer to access bid submissions and all related documents after bid closing.
C-06.04	for the Contracting Officer to provide evaluators with access to the technical bids.
C-06.05	for evaluators to document their results using pre-configured evaluation grids with embedded formulas.
C-06.06	for the Contracting Officer to divide the technical bid into sections for evaluation by multiple evaluators and assign to different team members.
C-06.07	for the Contracting Officer to set on/off permissions for collaboration between participants during the evaluation process.
C-06.08	to enable electronic communication between Contracting Officer and the designated contact person of the bidders who have submitted a bid to facilitate the exchange messages and transfer of files, documents etc. (e.g. request for clarification/documentation).
C-06.09	to compare and assess responses and capabilities of one or multiple suppliers against predefined questions.
C-06.10	to enable and support individual and consensus (team) evaluation process with ability to sequentially order, display and hide results and comments of each evaluator.
C-06.11	for the evaluator to save the bid evaluation results and continue work later before submitting final result of evaluation.

SOW NUM	Requirement
C-06.12	to export bid evaluation criteria and related weight factors to MS Excel spreadsheet.
C-06.13	for the Contracting Officer to perform automated and manual technical/financial evaluation and scoring based on selection and evaluation methodology, parameters and business rules predefined during the RFx creation.
C-06.14	to perform comparative evaluation of bids at the same time including, but not limited to, evaluation: a. on each item from a basket of goods b. group of items c. a whole basket of goods
C-06.15	for the Contracting Officer to configure the technical and financial evaluation to only evaluate certain items in the catalogue file in order to conduct a 'basket of goods' financial evaluation.
C-06.16	for the Contracting Officer to select and approve individual line items that a supplier is qualified for as a result of a technical and financial bid evaluation.
C-06.17	to calculate the final bid score based on RFx defined formulas and selection methodology.
C-06.18	to keep the financial envelope of technically non-responsive bidder locked (i.e. not to be opened).
C-06.19	to perform the evaluation of price items and determine a score per bidder, per item.
C-06.20	for evaluators to perform scenario analysis during bid evaluation (e.g. generate multiple optimization scenarios per sourcing event).
C-06.21	to support Bid Optimization scenario analysis by using various parameters and constraints including, but not limited to: a. non-financial criteria; b. matrices and tiers; and c. responses to RFx questions.
C-06.22	for the Contracting Officer to monitor current bid evaluation status.
C-06.23	for the Contracting Officer to generate an overall bid evaluation summary that includes: a. each stage of the bidding process; b. individual and overall suppliers scores; c. consensus results with comments by evaluators; d. qualitative and quantitative ranking; e. overall cycle time; and f. tabulated results of the ratings (as applicable to the RFx).
C-06.24	for the Contracting Officer to select and identify proposed winner(s) and notify all stakeholders of the result.

SOW NUM	Requirement
C-07.00	**Contract Award** The Contractor must deliver a solution that provides the functionality:
C-07.01	to validate that business rules for contract award are met prior to contract award including, but not limited to, ensuring mandatory documentation is on file and that the supplier is in good standing.
C-07.02	for the Contracting Officer to award contracts as a result of a competitive process.
C-07.03	for the Contracting Officer to award sole source contracts as a result of a non-competitive process: a. with reference to an RFx; b. without an RFx (direct contract creation).
C-07.04	for the Contracting Officer to create new contract by inheriting and copying information from an existing Model Contract.
C-07.05	for the Contracting Officer to add up to 99,999 line items to the contract.
C-07.06	to automate the process of moving the model contract from the published RFx to a final contract document.
C-07.07	for the Contracting Officer to configure contracting attributes (e.g. contract start date / end date, option period(s), optional services, contract limits and tolerance levels).
C-07.08	for the Contracting Officer to create contracts that include one or more pricing features (as selected by the user) including, but not limited to, firmed price, economic price adjustment, tier based price, cost reimbursable, fixed unit price, fixed time rate, with price adjustment, with fixed fee, with incentive fee, custom formula based.
C-07.09	for the Contracting Officer to create and manage various types of contracts including but not limited to one-off-contracts, multi-year and/or multi-phase contracts, Framework Agreements.
C-07.10	for the Contracting Officer to create and award multiple contracts, agreements and contractual documents against a single requisition and a single solicitation.
C-07.11	for the Contracting Officer to create and award one contract against multiple requisitions.
C-07.12	for the Contracting Officer to award one or multiple Contracts, Framework Agreements from a single solicitation process with multiple different permutations (e.g. different goods/services, delivery location, delivery method, etc.).
C-07.13	for the Contracting Officer to create, award and manage contract and contract related documents electronically.
C-07.14	for the Contracting Officer to award a contract to supplier by applying preconfigured business rules, formulas and algorithms from a Model Contract.
C-07.15	to publish and persist line item level contracts to the catalogue so that user can easily search and add those items to their shopping cart requisition.
C-07.16	for the Contracting Officer to delay, suppress or retract posting of Contract Award Notice and provide justification.

SOW NUM	Requirement
C-07.17	for the Contracting Officer to configure and publish Contract Award Notice on Government Electronic Tendering Service (GETS) once a contract is awarded and signed.
C-07.18	for the Contracting Officer to configure and send notices to bidders to advise them about outcome of the solicitation process (e.g. Letters of Regret).
C-07.19	to link the results of evaluation process to relevant contract award templates such as, but not limited to Letter of Regret, Contract Award Notice.
C-07.20	to create the list of users who will be receiving a notification of the contract award.
C-07.21	to assign a contract to multiple contracting authorities based on roles.
C-07.22	for the Contracting Officer to modify administrative contract elements (i.e. including, but not limited to, financial coding changes, contracting authority changes)through an automated approval workflow process.
C-07.23	for the Contracting Officer to retrieve and insert the clauses of the contract from the related RFx and not from the library.
C-08.00	**Contract Administration** The Contractor must deliver a solution that provides the functionality:
C-08.01	to enable electronic communication & collaboration between Contracting Officers and internal/external stakeholders to facilitate the process of collecting, sharing, and validating supplier related information (e.g. security validation, criminal record checks, etc.).
C-08.02	for the Contracting Officer to configure, create and monitor contract benchmarks and Key Performance Indicators (KPIs).
C-08.03	for the Contracting Officer to track, monitor, validate and manage contractual work progress and performance of the supplier.
C-08.04	to establish contract management milestones and bring forwards (BFs) at various stages of the contract (e.g. configuring auto notifications for contract milestones, transition periods, contract extensions).
C-08.05	for the Contracting Officer to configure triggers to facilitate the tracking and management of contractual events such as, but not limited to, deliverables and milestones due dates, validity period, renewal dates, Contractor reporting obligations, usage of funds, effort, under the contract.
C-08.06	for the Contracting Officer to manage contract amendment requests and all resulting changes to the contract.
C-08.07	for the Contracting Officer to create, approve, manage and control contract amendments.
C-08.08	for the Contracting Officer to activate, manage, and remove contract suspension including the resumption of work once the suspension has been lifted.
C-08.09	for the Contracting Officer to cancel/terminate a contract and update the status of published contract award notice on GETS (e.g. cancelled).

SOW NUM	Requirement
C-08.10	for the Contracting Officer to re-issue recurring contracts (i.e. contracts requiring renewal).
C-08.11	for the Contracting Officer to validate and record on file that contract deliverables are complete, invoices are paid, and all necessary documentation is on file before contract closure (e.g. contract close-out checklist).
C-09.00	**Project Management** The Contractor must deliver a solution that provides the functionality:
C-09.01	to enable the application of Project Management best practices that will allow user to create and manage procurement files by linking together all documents related to a sourcing event including, but not limited to: a. assignment of common unique identifier for linking requisition, contract and all associated procurement file documents; b. link all information related to the solicitation process and contract creation (i.e. evidence of approvals, risk assessments, procurement planning documents, requisition and any amendments); c. link all information related to the bid evaluation process (i.e. bid evaluation plan, resulting evaluation documents); d. link records of actions taken during a contract lifecycle (i.e. correspondence, records of phone discussions, formal records of meetings, meeting minutes, records of decisions); e. manage versions of all documents and templates during all phases of the Sourcing and Contract Lifecycle Management; and archive current and historical procurement file information.
C-09.02	to create dynamic process maps based on project attributes.
C-09.03	for the authorized administrators to configure and build dependencies within process tasks to ensure precursor tasks are completed before beginning others.
C-09.04	for the authorized administrators to create and manage multiple tasks within a process management tool.
C-09.05	for the authorized administrators to create and manage electronic forms that can be embedded into a process management tool.
C-09.06	for users to attach documents at the Project and Task level.
C-09.07	to support Process Management activities.
C-09.08	to support Document Management activities.
C-09.09	to support Knowledge Management activities.
C-09.10	to support Project/Activity Management.
C-09.11	to support Resource Management activities.

SOW NUM	Requirement
C-10.00	**Central Repository** The Contractor must deliver a solution that provides the functionality:
C-10-01	for the authorized administrators to create and manage a clause repository (library) in both official languages that can be accessed by Contracting Officer to create RFx, RFx amendments, Contracts, and contract amendments.
C-10-02	for the authorized administrators to identify corporate and custom clauses and designate clauses that require a workflow to be modified.
C-10-03	for the authorized administrators to configure and apply appropriate status to each clause throughout its lifecycle (e.g. Active, Superseded, Cancelled).
C-10-04	to support robust search capabilities of clause and conditions library (e.g. Keywords, dates, status, Clause ID etc...).
C-10-05	to link both versions (English and French) of the clause so that when a clause is referenced in the English version it is automatically referenced and/or updated in the French version or vise versa.
C-10-06	for the Contracting Officer to include full text and/or reference the clause in solicitation documents.
C-10-07	to keep accessible historic content of the clauses and conditions Library.
C-10-08	to make all versions of clauses and general conditions available publicly through the portal.
C-10-09	to notify Contracting Officer when the status of a referenced clause in the RFx changes and ensure the clause referenced in the RFx is copied to the final contract and not the updated version from the library.
C-10.10	for the authorized administrator and Contracting Officer to create and manage templates (e.g. present user with a list of standard steps to follow when creating new procurement template).
C-10-11	to identify usage and track changes made to a standard procurement template.
C-10-12	for the authorized administrators to configure the process to manage revisions to standard templates and clauses (e.g. rights to edit and manage clauses and templates libraries).
C-10-13	to enable authorized administrators to automatically update templates with the "Active" clauses.
C-10-14	to store cost formulas in repository as part of templates.

5.6 SECTION D: PROCUREMENT MANAGEMENT

5.6.1 Objectives of Procurement Management

The objective of the Ordering process within the e-Catalogue environment is to:

- Provide a 'Consumer-Like' experience to a casual user, which will guide the user through the Ordering Process, while ensuring that the eventual Order is in full compliance with the Framework Agreement
- Reduce the risk of the user ordering the incorrect product or service
- Provide a 'one stop' online store for users to search electronic catalogues for and view approved goods and services though a Framework Agreement established by the GC
- Apply and enforce business and financial rules and approvals to Orders
- Ensure compliance to terms and conditions of Framework Agreements

- Electronically submit Shopping Cart Requests and Orders to Suppliers from EPS
- Facilitate flow of transactional communication between the Supplier and the GC
- Maintain an audit trail of all transactions
- Provide full reporting and monitoring functionality

5.6.2 Background Information on Framework Agreements

The GC has a number of existing Methods of Supply that it has established; particularly for the procurement of Mandatory Standing Offers and Supply Arrangements which it will continue to maintain and may be updated over time. The GC will continue to establish new Methods of Supply as needs arise based on its continued strategic review of procurement requirements, spend analysis and historical trends.

PWGSC is the only GC organization that can establish Framework Agreements that can be used by other GC organizations, as well as the broader Canadian Public Sector (Provinces, Municipalities, etc). Any GC Organization can establish a Framework Agreement for their own use with the exception of the Mandatory Standing Offers and Supply Arrangements.

As the GC buys a diverse range of goods and services, the GC establishes Framework Agreements for these, including but not limited to:

- Armament
- Audit Services
- Engineering Services
- Audio Visual Equipment
- Clothing & Textile
- Commercial Training
- Communication Services
- Environmental Remediation Services
- Environmental Services
- Food & Beverage
- Furniture
- Informatics Professional Services
- Janitorial Services
- Language Training
- Medical Equipment & Supplies

- Non-IT Services
- Office Equipment
- Office Furniture
- Office Seating
- Office Supplies
- Pharmaceuticals
- Research & Development Services
- Software
- Temporary Help Services (Contingent Labour)
- Training Development & Delivery Services
- Translation Services
- Vehicles (Purchase, Lease, and Rental)

As part of the GC Open Data initiative, PWGSC publishes all the active Standing Offers and Supply Arrangements that are issued by PWGSC, which is available here: https://buyandsell.gc.ca/procurement-data/standing-offers-and-supply-arrangements/download-sosa-data. This data does not include Contracts with Task Authorizations or Standing Offers & Supply Arrangements issued by Government Departments other than PWGSC.

5.6.2.1 Framework Agreement Types

Depending upon the overarching Method(s) of Supply [and Framework Agreement(s)] which inform the particular e-Catalogue, an e-Catalogue may take one of the following forms:

- Simple/Configurable e-Catalogue(s) – which must allow GC users to browse, select and request goods and/or services that are either pre-set (i.e. defined) at a unit price; or are configurable where the GC user can select from among available options for the goods and/or service (e.g. colour, size, etc.) at a unit price(s).

- Complex e-Catalogue(s) – which will allow GC users to browse, select and request more complex goods and/or services. In a complex catalogue, the GC user will need to develop and send to the pre-qualified Supplier(s) a Statement of Work (SOW), to which the pre-qualified Supplier(s) will be required to respond before an Order may be placed. In some cases, these complex e-Catalogues may require a second-stage selection process to be conducted (refer to e-Sourcing below).

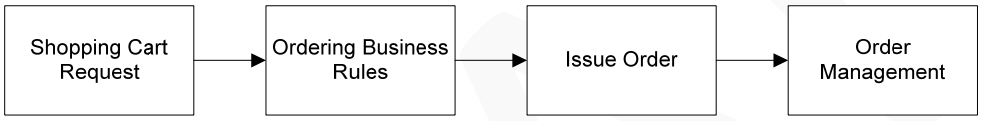
For requirements that require a second-stage selection process (using the Supply Arrangement), a more formal RFx process will be initiated based on the applicable business rules.

EPS must provide activation/deactivation of catalogues base on a Framework Agreement validity period. The functionality must include management of pre-qualified Supplier resource information (e.g. capture and updating of qualifications, credentials, etc.) for professional services resources; recording, monitoring, reporting and taking action on the performance of pre-qualified suppliers and resources.

5.6.2.2 Ordering Process

When a need is identified, a user will typically first search the e-Catalogue to determine if there is a Framework Agreement with the good(s) and/or service(s) they are seeking. As the GC has thousands of Framework Agreements with a large number of goods and services, the user must be able to easily navigate and find the goods and services they are trying to acquire amongst all of the Framework Agreements.

Where an item is available, a GC user may then select the items and add them to a Shopping Cart, which triggers, through business rules, requirements for review and approval by other GC users (e.g. management approval of budget, authority to enter into the Contract, Legal Review, Functional Authority approval, etc.) and a Shopping Cart request is sent to the applicable suppliers based upon the applicable business rules (Ordering Business Rules) of the particular Framework Agreement to either confirm availability of the Supplier to complete the Order or to have the Supplier submit a proposal (e.g. proposed resource's CV, price for installation) for evaluation by the GC. The Ordering Process continues by issuing the Order to the selected Supplier(s) in accordance with the business rules, with the Order being managed to completion.



The Procurement Management functionality must support collaboration and communication between GC users and pre-qualified Suppliers in the management of Orders placed against the established e-Catalogues, including recording, monitoring, tracking, reporting and enabling GC users to take action on delivery status and performance of Suppliers against Orders (e.g. on time, on budget, right quality, etc.); to amend Orders (e.g. increase/decrease quantity, change delivery date, etc.); and enable Suppliers to submit timesheets, invoices, and other supporting documentation to facilitate the management and close-out of the Order.

5.6.3 Ordering Business Rules

Ordering Business Rules are business rules for ensuring openness, fairness, transparency and integrity of the Ordering Process for multi-Supplier sourced Methods of Supply that provides the built-in controls to respect the Terms & Conditions of the Method of Supply in order to ensure that the Orders are issued in an objective manner which meets the socio-economic objective of the GC including:

- Reducing barriers to small and medium enterprise business by providing them an equal opportunity to compete with larger firms;
- Respecting all legislation, regulations, policy and ensuing a fair distribution of Orders amongst the qualified Suppliers for the applicable Method of Supply for the selected goods and services;
- Provides best value to the GC;
- Enhancing the integrity and efficiency of the acquisition process.

5.6.4 Two-Stage Procurement Rules (Supplier Selection Methodologies)

For Framework Agreements that require a second-stage selection process (e.g. Supply Arrangements), as there is a second stage of competition, the solution is required to support the

Supplier Selection Methodologies. These methodologies are used to determine: the minimum number of eligible pre-qualified Suppliers to be invited, the minimum number of calendar days for the RFx posting, how Suppliers are selected (e.g. random, rotational) and the Publishing requirements (e.g. direct invitation vs. published on GETS). Typically there are different rules (tiers) based on dollar value.

The second stage typically requires a competitive RFx to be created as outlined in the e-Sourcing requirements.

5.6.5 Establishment of Framework Agreements

Framework Agreements are established by GC users with administrative rights who will establish the structure and configuration options for the contents of each Framework Agreements. Framework Agreements are created following the conclusion of a Sourcing Event that results in the awarding of one or more Framework Agreements to one or more Suppliers. Framework Agreements are designed to support the easy acquisition of the transactional goods and services required by clients; while at the same time leveraging the GC buying power, and helping the GC achieve a number of socio-economic objectives, including: supporting Small and Medium Enterprises, Aboriginal businesses, and Land Claim Areas. Framework Agreements presently include Standing Offers (SOs), Contracts with Task Authorizations (TAs), and Supply Arrangements (SAs).

For the Sourcing Event to establish the resulting Framework Agreement, the Contracting Officer will create a Catalogue Data File using the applicable catalogue attributes (e.g. Part #, Item Description, Price). Once the structure is created, the Contracting Officer will then populate the Catalogue Data File with the goods and services that Suppliers will be required to bid on during the Sourcing Event. Depending on the requirements of the Sourcing Event, the Suppliers will either be required to submit pricing on all items or have the option to submit pricing on select items. The Contracting Officer will either use GC created content, content acquired by 3rd party data aggregators, supplier provided information or a combination thereof. As a result of the evaluation process (Technical and Financial) during the Sourcing Event, the information (some or all) of the Suppliers who are issued a Framework Agreement will then be made available for users to access. It is important that the applicable information persists from the Sourcing Event to the e-Catalogue area without requiring the information to be extracted from the system, manipulated and then imported to the e-Catalogue.

The Framework Agreement (created as a result of a Sourcing Event) can have either a fixed or an unlimited number of Suppliers. Typically, the GC will issue multiple supplier Framework Agreements to ensure that the GC has access to a sufficient source of supply and to achieve socio-economic objectives, such as ensuring that Small and Medium Enterprises can compete for GC business. Framework Agreements can be issued for a Single Organization for a single Region (e.g. for Department of National Defence in Halifax) up to being issued for Multiple Organizations for Multiple Regions (e.g. available for all of the GC in Ontario and Quebec)

When creating the Framework Agreement, the Contracting Officer will need the functionality to set the Method of Supply attributes in the e-Catalogue area in order to ensure the applicable Business Rules are followed. Method of Supply attributes may include, but are not limited to: Ordering

Business Rules which govern how Shopping Cart Requests are distributed to the eligible Suppliers for the eventual placement of subsequent Orders against the Framework Agreement; Client Order Limitation for an individual Order; GC Order Limitation for an individual order; the limitation on the value of Orders which may be placed to an individual Supplier (if applicable for the Method of Supply) and the cumulative limitation for all Suppliers on the Method of Supply (if applicable for the Method of Supply); validity period of the Method of Supply (start date, end date, option periods) (e.g. validity of price); terms and conditions for the Orders; setting the Authorized Users and Authorized Organizations.

Information on the goods and services offered by each Supplier will be provided either pursuant to the original Sourcing Event or as a result of a subsequent update to the Supplier's goods and services offerings. In some cases, the functionality of the EPS will allow the Supplier to provide incremental catalogue updates to their offerings, or certain aspects of their offerings, dynamically, or in response to a collaborative request from a GC user.

5.6.6 Requirements

Table 99 – Procurement Management Requirements

SOW NUM	Requirement
D-01.00	**General - General** The Contractor must deliver a solution that provides the functionality:
D-01.01	for authorized administrators to configure and manage all business rules as administrative functions by central and distributed administrators.
D-01.02	to allow users to group related Contracts and Orders together.
D-01.03	for the user to view and display the workflow history for all ordering processes
D-01.04	for users to view buyer and supplier details via hyperlinks in order to access their information at any point by clicking or hovering over a link.
D-01.05	for users to search Shopping Cart requests and Orders based on reportable fields.
D-01.06	for authorized administrators to configure the Shopping Cart requests and order forms, including determining which fields are included and which data is displayed and the sort order to be used in one or more Catalogues.
D-01.07	for authorized administrators to configure the order status, which reflects the stage of the ordering process it is in (e.g. draft submitted, approved, ordered, received).
D-02.00	**Catalogue - General** The Contractor must deliver a solution that provides the functionality:
D-02.01	for suppliers and authorized administrators to input and manage Catalogue content for goods and services (e.g. product numbers, pictures and descriptions, Method of Supply).
D-02.02	for Catalogue content to be displayed in the language in which it was recorded or in the preferred language of the user, if the catalogue content is available in both languages.
D-02.03	to support access to PunchOut Catalogues.

SOW NUM	Requirement
D-02.04	to export Catalogue File into other different file formats in order to allow an user to manipulate the Catalogue File work off-line and to import it back into EPS.
D-02.05	to convert Catalogue prices that are in a foreign currency to Canadian dollars using the applicable exchange rate from the Bank of Canada as of the specified date and time by the user in order to evaluate the Catalogue prices in Canadian dollars and either keep the Catalogue prices in the original currency or the converted Canadian currency.
D-03.00	**Catalogue - Creation** The Contractor must deliver a solution that provides the functionality:
D-03.01	for authorized administrators to create simple, complex, and configurable Catalogues for goods/services based on Method of Supply attributes, where the authorized administrator configures if the supplier is required to send additional information before an order can be issued (e.g. user selects a TV from a catalogue but requires the Supplier to quote a price for Installation services or provide a CV for a proposed resource).
D-03.02	to create the configuration options for a configurable Catalogue item to be selected by the user in the Shopping Cart (e.g. building a laptop, vehicle).
D-03.03	to manage Method of Supply attributes for an individual Catalogue and ensure they are applied during the ordering process (e.g. authorized administrators, authorized organizations, regions, Ordering Business Rules, Order thresholds, Method of Supply limitation (individual supplier limitation and cumulative limitation for the Method of Supply), terms and conditions, Comprehensive Land Claims Agreements, Set aside for aboriginal business).
D-03.04	to create and manage different Client Organization and PWGSC order thresholds for different Catalogues.
D-03.05	to configure the issue of an Order with a delivery date/end date that extends beyond the end date of the Method of Supply.
D-03.06	for authorized administrators to create configurable standard terms and conditions within a clause library for their Method of Supply in order for a user to select the appropriate clause(s) during the ordering process.
D-03.07	to manage information about the Method of Supply (e.g. product help, Catalogue background information, help details for the Method of Supply) within the Catalogue.
D-03.08	for authorized administrators to configure restrictions on the data entry of price in the Catalogue File (e.g. decimal precision, maximum price, minimum price).
D-03.09	to support an unlimited number of Catalogues.
D-03.10	to allow authorized administrators to configure the data fields in a Catalogue File that a Supplier can edit within the solution.
D-03.11	for authorized administrators to authorize the viewing and access of Catalogue information by user role and permissions.

SOW NUM	Requirement
D-03.12	for authorized administrators to configure for their Catalogue the Shopping Cart in order to include only the relevant data fields (e.g. supplier part number, description, Unit of Measure, unit price, calculated total price, need-by-date, payment & shipping terms) associated to their Catalogue in order to ensure only the relevant fields are displayed to the user.
D-03.13	for authorized administrators to configure if a supplier can accept or reject, with comments, a Shopping Cart request.
D-03.14	for an authorized administrator to configure the notification thresholds (e.g. percentage or dollar amount) of the individual supplier limitation and cumulative limitation for the Method of Supply when the dollar amount of orders issued reaches the applicable threshold.
D-03.15	for authorized administrators to enter System Enabled Supplier Card (Ghost Card) Information in each individual Catalogue File in order to utilize in an Order that will be paid by a credit card.
D-04.00	**Catalogue - Data Management** The Contractor must deliver a solution that provides the functionality:
D-04.01	for authorized administrators to map commodity codes to general ledger accounts.
D-04.02	for authorized administrators to create and manage master unit of measures to be used in the Catalogue file (e.g. box, pallet, metric).
D-04.03	for authorized administrators to create and manage master list of Regions and descriptions to be used in the Catalogue file.
D-04.04	for authorized administrators to create and manage master list of Methods of Payments and Basis of Payment and descriptions to be used in the Catalogue file (e.g. Per diem, ceiling price, fixed price, single payment, monthly payment, milestone payment, cost reimbursable).
D-05.00	**Catalogue - Catalogue File** The Contractor must deliver a solution that provides the functionality:
D-05.01	for authorized administrators to create, search, manage, sort, and filter a master list of attributes in both Official Languages of different types (e.g. yes/no, memo, date, currency, number, percentage, picture, custom) that can be used as attributes in a Catalogue File.
D-05.02	for authorized administrators to search, sort, and filter in order to select and manage the attributes from the master attribute list.
D-05.03	for authorized administrators to configure minimum order values on a line item and order basis, for goods and services in a given Catalogue, in order to enforce the restrictions during the ordering process and to notify the user who is placing the order of the restrictions.
D-05.04	for authorized administrators to create an identifier link to indicate items that are equivalent (same fit, form, and function) to each other.
D-05.05	to support the creation and management of an unlimited number of line items within a Catalogue.

SOW NUM	Requirement
D-05.06	to group items into mandatory bundles where items cannot be removed by the user (e.g. Microsoft Office on a computer).
D-05.07	to group items into optional bundles where select items can be removed by the user (e.g. extended warranty on a product).
D-05.08	to group together related variants of a specific item according to configurable attributes (e.g. colour, size).
D-05.09	to include multiple pictures (e.g. different views) per Catalogue line item.
D-05.10	to include a 360 degree model for a Catalogue item.
D-06.00	**Catalogue - Pricing** The Contractor must deliver a solution that provides the functionality:
D-06.01	for a wide variety of pricing attributes including but limited to fixed price, time and material, ceiling price, discount schedule, and cost plus.
D-06.02	to identify the currency of the pricing attribute(s) of a Catalogue File.
D-06.03	to provide different prices for multiple regions in a Catalogue File.
D-06.04	for authorized administrators to schedule the frequency (e.g. daily, monthly, on a specific date) to connect to the applicable commodity index feed in order to update the prices in the Catalogue File based on a markup or discount pricing attribute.
D-06.05	for authorized administrators to configure and manage tiered price ranges for items on each Catalogue File that are used to determine pricing on an individual order.
D-06.06	for authorized administrators to configure and manage cumulative tiered price ranges that are applied to an individual order for items in a Catalogue File (e.g. tiered price would become available to a user based on cumulative orders).
D-06.07	for authorized administrators to configure and manage bulk tiered price ranges that apply a discount to an individual order for a Catalogue File (e.g. the entire order is discounted based on a dollar amount).
D-06.08	for authorized administrators to update the Manufacturer Suggested Retail Price (MSRP), apply the supplier markup/discount, and display the final price to the user.
D-06.09	for authorized administrators to manage and update the price list information for Catalogue Files on a dynamic basis.
D-06.10	to connect to the applicable Consumer Price Index (CPI) table from Statistics Canada to determine the price update calculation when required by a given contract / framework agreement.
D-07.00	**Catalogue - Management** The Contractor must deliver a solution that provides the functionality:
D-07.01	for authorized administrators to examine, manage, verify and approve Catalogue information within the solution.
D-07.02	for authorized administrators to browse, search, sort, and filter any field within a Catalogue File.
D-07.03	for version control of a Catalogue File and to display the version number and date of the Catalogue File.

SOW NUM	Requirement
D-07.04	for authorized administrators to search (e.g. by supplier, product, date) for previous Catalogue File versions.
D-07.05	for authorized administrators to compare the new and previous Catalogue File versions and determine changes made.
D-07.06	for authorized administrators to use any version of the Catalogue File for a future update.
D-07.07	for authorized administrators to add/remove/update any record within a Catalogue File.
D-07.08	for suppliers to request an update for an existing Catalogue item.
D-07.09	for authorized administrators to schedule the effective date/time when an initial Catalogue or updated Catalogue is published (both with Method of Supply and individual Catalogue File level) for client use.
D-07.10	for suppliers to download a locked spreadsheet with configurable editable fields in order to restrict which information can be changed by the Supplier, and to allow Suppliers to upload the Catalogue changes into the system for approval within a secure environment.
D-07.11	for authorized administrators to configure thresholds and predefined conditions for auto-approval of both items and price changes to a Catalogue File and to initiate a separate approval process for those updates that are outside of the pre-defined conditions in order to approve individual or bulk item updates to the Catalogue File, and to notify the appropriate users of the changes made.
D-07.12	to apply a pre-defined pricing evaluation framework of the Catalogue Files in a Catalogue and to allow for a review by an authorized administrator to ensure that the pricing is in accordance is with the pricing evaluation framework.
D-07.13	for authorized administrators to configure when a user is notified when a Catalogue or Catalogue item has not been updated for a configurable period of time.
D-07.14	for authorized administrators to deactivate, activate, or suspend specific items in one or more Catalogue Files in a Method of Supply.
D-07.15	for authorized GC administrators to import and upload Catalogue updates on behalf of the supplier.
D-07.16	for suppliers to update Catalogue data through an automated self service standard data upload integration through web services or Electronic Data Interface.
D-07.17	to determine continued compliance of a supplier under an awarded Framework Agreement to provide goods and services (e.g. security, clearance) and to notify a user when they are no longer in compliance.
D-07.18	for when a Method of Supply end date has passed, to deactivate the related Catalogue File.
D-07.19	to identify and manage unique Catalogue line items in the Item Master Record file to prevent duplication of Catalogue items.
D-08.00	**Shopping Cart - General** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
D-08.01	for authorized administrators to create a Shopping Cart request on behalf of another user and client department.
D-08.02	to create a unique number structure (with prefix/suffix) for a Shopping Cart request that carries forward to an Order and which can be used for tracking various versions of the same Shopping Cart request.
D-08.03	to assign a unique Shopping Cart number using the number structure when a Shopping Cart request is sent to a supplier or workflow approval.
D-08.04	to compare Catalogue items according to their specifications (e.g. price, size, weight, benchmark evaluation).
D-08.05	to calculate the distance (air, or ground using existing infrastructure, not "as the crow flies") between multiple points to determine the overall cost (e.g. number of KMs times cost per KM).
D-08.06	for additional information about an item (e.g. moving to and from, comments, restrictions) to be specified via a web form.
D-08.07	to determine the price according to the address of the delivery location.
D-08.08	for users to collaboratively work with suppliers on defined Shopping Cart items through a configurable form (e.g. for services requirements).
D-08.09	to allow suppliers to submit the content of their response to a Shopping Cart request until the configurable response deadline.
D-08.10	to allow a purchase of a good or service for a lower price than what is stated in the Catalogue.
D-08.11	to set Method of Supply Limitations by periods.
D-08.12	to ensure that Shopping Cart requests and Orders do not exceed the maximum Method of Supply Limitation (e.g. Contract value).
D-08.13	to provide a configurable print layout of the Shopping Cart request.
D-09.00	**Shopping Cart - Search** The Contractor must deliver a solution that provides the functionality:
D-09.01	for authorized administrators to configure faceted search elements for each Catalogue File.
D-09.02	for users to perform searches that will find matches even when users misspell words or enter in only partial words for the search (commonly called "fuzzy logic searches").
D-09.03	for users to conduct a federated search of all Catalogue content in a single executed search, excluding Punch-Out Catalogue.
D-09.04	for users to perform an advanced Boolean Catalogue search.
D-09.05	for users to conduct a federated search of all Catalogue content in a single executed search, including Punch-Out Catalogue.
D-09.06	for users to navigate Catalogue content via a category driven hierarchy.
D-09.07	for users to search for a good or service within a specified price range.
D-09.08	to filter eligible Catalogue suppliers that meet a selected socio-economic condition in accordance with their Supplier Relationship Management Profile (e.g. Aboriginal).
D-09.09	to display the attributes for the applicable Catalogue Item.

SOW NUM	Requirement
D-09.10	for a cross-PunchOut search for an item.
D-09.11	for users to save a previously executed search for future use (e.g. bookmark).
D-09.12	to suggest complementary or related products/services (cross-selling) that are brand agnostic for the user's selected goods or service (e.g. laptop would suggest a bag, warranty, installation service).
D-10.00	**Shopping Cart - Creation** The Contractor must deliver a solution that provides the functionality:
D-10.01	for users to select various options of the same product with some varying attributes (e.g. colour).
D-10.02	to determine the price of each item, taking into account all taxes, duties/customs, discounts, business rules, and shipping costs, and to calculate the total cost in relation to these factors.
D-10.03	at the header level and for each line item for users to input multiple financial codes, delivery addresses (including free-form Attention line field), delivery schedules, delivery instructions, invoice addresses.
D-10.04	for users to input a maximum requested value for budget approval of a Shopping Cart request.
D-10.05	for users to select the method of payment type from the approved types which were configured by the authorized administrators at the Catalogue level.
D-10.06	for users to select a delivery address from an official master list and provide the ability for the user to enter in a ship-to address that is not included in the official master list which would require a separate configured approval workflow (e.g. This would be used to enable Remote Workers to ship to their home or satellite offices.).
D-10.07	to provide intelligent defaulting of financial codes based on user, department, supplier, commodity, item, or any combination thereof on the Shopping Cart request line item.
D-10.08	to identify a Shopping Cart request as either a capital asset or an operating expense based on at least one of the following methods: - user selection - GL Account - Commodity Code
D-10.09	for users to execute a "Quick Quote" with selected Suppliers for purchases under an identified dollar threshold or commodity where more than one supplier exists prior to submitting Shopping Cart request for approval and eventual purchase order.
D-10.10	for users to attach notes and supporting documents (including ZIP folders) and designate the document as "internal" to the overall Shopping Cart request and to each line item (as applicable) to support the approval process that can be assigned to certain fields (e.g. Security Requirement Check List (SRCL) document can be attached to an SRCL field).

SOW NUM	Requirement
D-10.11	for users to attach supporting documents (including ZIP folders) to the overall Shopping Cart request and designate the document as "Supplier" to be sent to the supplier once approved (e.g. Word documents, media files, CAD drawings, spreadsheets) that can be assigned to certain fields (e.g. Security Requirement Check List (SRCL) document can be attached to an SRCL field).
D-10.12	to allocate a Shopping Cart request against a specific fiscal year period and ensure that it can be allocated at the item level or order level.
D-10.13	for authorized administrators to configure a form (e.g. Web form) for a specific Method of Supply using the applicable Catalogue attributes, that a user will complete as a means to determine the list of suppliers that are eligible to provide the good or service in order to commence the Ordering Process, including the use of the applicable Ordering Business Rules (e.g. the User selecting the security clearance level for a resource).
D-10.14	to alert users in the event that their Shopping Cart request exceeds the maximum threshold of an individual Method of Supply and prevent the user from submitting the request.
D-10.15	to inherit fields from the Shopping Cart request to an Order.
D-10.16	for quantities of the same item on the same order line to be delivered at different times and locations.
D-10.17	for users to select an authorized dealer, reseller, or agent when ordering a good or services (e.g. vehicles).
D-10.18	to have the supplier select an authorized dealer, reseller, or agent of a good or service (e.g. vehicles) nearest the postal code of the delivery location if one is not specified by the client.
D-10.19	to automatically validate that items within a Shopping Cart are still valid to be purchased in the Catalogue. (e.g. item discontinued by a supplier, or supplier no longer exists, the system validates that the product no longer exists so Shopping Carts cannot proceed).
D-10.20	for users to select a configurable item based on the configurable elements in the Catalogue to create a Shopping Cart request (e.g. Selecting the computer type, components, etc. in order to determine eligible suppliers).
D-10.21	for authorized administrators to configure if a user can select specific clauses related to an Order (e.g. Method of Payment is Single Payment or Monthly Payments).
D-10.22	for users to receive item level shopping details from a PunchOut Catalogue.
D-10.23	to allow users to select items from different Catalogues and apply the applicable Ordering Business Rules to the related Catalogue(s).
D-10.24	to determine the Canadian dollar equivalent for Shopping Cart requests that have Catalogue items not using the Canadian currency using the applicable exchange rate from the Bank of Canada in order to be used throughout the applicable approval process.
D-10.25	to create a Shopping Cart request by executing a search of the Catalogue content and selecting items.

SOW NUM	Requirement
D-10.26	for users to initiate, on the same screen, a non-Catalogue requisition upon a search for items not present in the Catalogue.
D-11.00	**Shopping Cart - Display** The Contractor must deliver a solution that provides the functionality:
D-11.01	to display to users the applicable attributes of a Method of Supply when Shopping.
D-11.02	to display products recently viewed by the user.
D-11.03	to group together items according to similar product variants.
D-11.04	to display a single page summary screen of the Shopping Cart request for workflow approval and prior to submitting it to a Supplier.
D-11.05	to include thumbnail pictures as part of a Catalogue search result.
D-11.06	to allow comparative shopping in a side by side comparison.
D-11.07	to display the base price of a good or service before additional features are selected.
D-11.08	to display the price of Catalogue items that is not in Canadian Currency in both the Foreign Currency and the Canadian dollar equivalent using the applicable current exchange rate from the Bank of Canada.
D-12.00	**Shopping Cart - Inventory** The Contractor must deliver a solution that provides the functionality:
D-12.01	for suppliers to update goods or service availability status configured to update on a real time, scheduled batch, or manual basis.
D-13.00	**Shopping Cart - Management** The Contractor must deliver a solution that provides the functionality:
D-13.01	for users to identify specific Catalogue items as favourites for future use.
D-13.02	for users to edit a non-catalogue requisition item and replace with an existing catalogue item(s) and re-route to the applicable workflow.
D-13.03	For users to change any element in the Shopping Cart (e.g. the quantity of items ordered, delivery date and shipping address) prior to placing the order.
D-13.04	for users to update old Shopping Cart requests to generate a new Shopping Cart request.
D-13.05	for users to save the Shopping Cart for later retrieval.
D-13.06	for users to copy an existing Order and create an editable Shopping Cart request accessible by a select set of users.
D-13.07	for users to create a Shopping Cart request with a standard order to be made at scheduled intervals (e.g. monthly paper order).
D-13.08	for the solution and/or user to queue multiple Shopping Cart requests from one or more users across multi organizations into one Shopping Cart request based on configurable Catalogue business rules that trigger the release of the Shopping Cart request (e.g. deliverable date, lead time, geographic location, client department, tiered pricing) in order to take advantage of tiered pricing, or request for volume discounts (e.g. Reverse eAuctions).
D-14.00	**Shopping Cart - Taxes** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
D-14.01	to calculate the taxes in accordance with Canadian tax laws.
D-15.00	**Ordering Business Rules - General** The Contractor must deliver a solution that provides the functionality:
D-15.01	for users to see the historical progress of a Shopping Cart request throughout the Ordering Process.
D-15.02	for suppliers to withdraw a response to a Shopping Cart request up to the time of order issuance.
D-15.03	for authorized administrators to configure the default maximum order response period (in working days) a supplier has to respond to the Shopping Cart request.
D-15.04	to allow users to view a supplier response to a Shopping Cart request and evaluate the response if necessary, and either reject the response with comments, or create an order and issue it to the supplier.
D-15.05	for authorized administrators to configure a collaboration form for a Shopping Cart Request for a Catalogue item that requires collaboration with a Supplier (e.g. user selects a TV from a catalogue but requires the Supplier to quote a price for Installation services).
D-16.00	**Two-Stage Procurement Rules** The Contractor must deliver a solution that provides the functionality:
D-16.01	for authorized administrators to configure business rules for sourcing events under individual Supply Arrangements with respect to the number of suppliers invited, how the suppliers are selected (e.g. random, user pick, combination, all), and the minimum number of calendar days for the bidding period based on different ranges of dollar amounts (e.g. Tiered Business Rules).
D-16.02	for users to configure a deadline for the submission of a bid according to a Method of Supply business rule.
D-16.03	for users to view a list of eligible pre-qualified suppliers based on sourcing rules under a Supply Arrangement.
D-16.04	for users to publish solicitation documents in a reserved area for only invited suppliers to view, with the configurability for the user to translate it into the suppliers' preferred language.
D-16.05	for users to add suppliers to the invitation for a 2-stage procurement RFx while it is available to be bid on.
D-17.00	**Ordering - General** The Contractor must deliver a solution that provides the functionality:
D-17.01	for users to display the total order price taking into account all applicable costs and discounts.
D-17.02	for users to save, modify or cancel orders at any time up to settlement.
D-17.03	to notify the appropriate users of an order rejection and a reason why (e.g. insufficient resources to complete the order, delivery issues).
D-17.04	to restrict visibility and access to existing orders based on user roles.
D-17.05	to ensure all Orders are tracked against the applicable Method of Supply.

SOW NUM	Requirement
D-17.06	to configure the numbering structure for amendments made to an Order using the original Order number as a baseline.
D-17.07	to ensure for any order, including outstanding orders, the order information relates to the appropriate version of the Catalogue File.
D-17.08	to issue the Order in the applicable currencies of the Catalogue.
D-18.00	**Ordering - Creation** The Contractor must deliver a solution that provides the functionality:
D-18.01	to restrict the users' ability to issue an Order based on the user profile or the specific commodity.
D-18.02	to split a Shopping Cart request into multiple Orders, as required, based on the results of the Ordering Business Rules.
D-18.03	to split a Shopping Cart request into multiple Orders based on any data element on the Shopping Cart request line item (e.g. Ship to, client organization).
D-18.04	for users to configure what additional information will be provided by the supplier (e.g. delivery date, prices, discounts, charges, and item classification codes).
D-18.05	to alert the users, in the event the order they are creating, exceeds the spending limit against an individual Method of Supply, and prevent the user from creating the Order.
D-18.06	to issue the Order to the supplier and to the clients' departmental financial management system, and to notify the user the Order has been issued, and to any other stakeholder in the workflow process (e.g. sending order information that have security requirements to CISD).
D-18.07	to notify applicable users that an Order could not be successfully transmitted, and provide the functionality for the user to resend the Order.
D-18.08	for authorized administrators to configure a percentage variance for individual Method of Supply that can be applied to an overall Order to account for the estimated order amount and the actual (e.g. fuel delivery exceed variance of 5%) in the applicable Catalogue.
D-18.09	for users to request approval to order more than the client order threshold and their delegation of authority.
D-18.10	for users to review previous rates paid for selected geographical locations and categories and sub-categories during the ordering process.
D-18.11	for users to negotiate the price with the selected supplier during the ordering process when the associated good or service has a ceiling price.
D-19.00	**Ordering - Management** The Contractor must deliver a solution that provides the functionality:
D-19.01	for users to configure the print layout and print an Order.
D-19.02	for users to request a Change Order.
D-19.03	for a workflow process based on a Method of Supply, to terminate an Order and indicate the termination reason through a pre-configured selectable list of reasons (e.g. default, mutual consent, for convenience of the Crown) along with supporting documentation.

SOW NUM	Requirement
D-19.04	for the supplier to provide the client through the system with initial shipment details (e.g. Tracking number, method of transport, estimated delivery time, goods information) and updated shipment details as required.
D-19.05	to receive line level information on Goods receipt and Invoice data from the departmental financial management systems.
D-19.06	for users to notify the supplier of the condition of the goods received, at the line item level, by selecting from a configurable list of conditions and free-form text information (e.g. report received good, report shortages, damaged items).
D-19.07	for suppliers to identify the name(s) of the country or countries of the goods' origin regardless of whether the work is to be performed by the supplier or one of its subcontractors.
D-19.08	for users to display the history of changes of terms and conditions.
D-19.09	for authorized administrators to configure if a supplier can accept or reject, with comments, a Change Order request.
D-20.00	**Ordering - Display** The Contractor must deliver a solution that provides the functionality:
D-20.01	for authorized administrators to configure a display of an order summary.
D-20.02	for users to view the Catalogue item associated to any document throughout the Order process.
D-20.03	to configure the Context-sensitive User Interface behaviour for a form based on the step made during the Ordering process and the configuration of the Method of Supply (e.g. After the supplier accepts and order, the user will see the Amend Order button, but not before).
D-20.04	for users to view and drill down all Shopping Cart requests tied to an Order.
D-20.05	to display the payment method (System Enabled Supplier Card vs. Invoice) and the related information (e.g. credit card number, invoicing instructions) on the Order.
D-21.00	**Reverse eAuction - General** The Contractor must deliver a solution that provides the functionality:
D-21.01	to allow suppliers to update their bids during the course of the auction event.
D-21.02	to allow suppliers to select individual Reverse eAuctions for instant email notifications about any changes to a Reverse eAuction (e.g. New bid, time extended, Reverse eAuction terminated).
D-21.03	to ensure that suppliers cannot submit a bid after a Reverse eAuction event has closed.
D-21.04	for suppliers to submit questions in relation to a Reverse eAuction event and for the user to meta tag the question and to publish and edit the question and response in both official languages during the Reverse eAuction event for all suppliers to view (e.g. Q/A form) without the supplier name being published.
D-21.05	for Suppliers during a preview period of a Reverse eAcution event to set both their opening bid and their maximum bid threshold in order to allow for an automatic bid to be placed in accordance with the bid increments.

SOW NUM	Requirement
D-21.06	to provide the user with a Reverse eAuction summary upon the completion of an event, including: final event details, quote activity, estimated savings, and event notes.
D-22.00	**Reverse eAuction - User Interface** The Contractor must deliver a solution that provides the functionality:
D-22.01	to display an event countdown clock of the time remaining for a Reverse eAuction event.
D-22.02	to automatically update the Reverse eAuction displayed information without requiring the user to refresh the page.
D-22.03	to display the results of a Reverse eAuction event to include which suppliers were invited, who participated, the rankings of participating bidders, the winning bid, and the total value of the contract/order.
D-23.00	**Reverse eAuction - Auction Creation** The Contractor must deliver a solution that provides the functionality:
D-23.01	to allow users to create, manage, and cancel Reverse eAuction events.
D-23.02	to allow users to configure the Reverse eAuction to be either open to suppliers as a public event (open to all suppliers), to a list of pre-qualified suppliers under a Method of Supply, or to a list of selected suppliers.
D-23.03	to allow users to configure the calculated ranking of the individual item(s) or lot(s) for a Reverse eAuction event in order to determine the winner of the individual item(s) or lot(s).
D-23.04	to allow users to configure whether the winning bid will be issued as an order against a Method of Supply or as a contract against a RFx.
D-23.05	to allow users to configure the currency used for a Reverse eAuction event in which a supplier must submit their bid.
D-23.06	to allow users to configure the bid increment, by a percentage or a dollar amount, for a Reverse eAuction event.
D-23.07	to allow users to configure for an individual Reverse eAuction event the visibility rules for suppliers to see all pricing and rankings, or to see only the rankings for a bid; and to display the actual supplier name or assign a generic supplier name (e.g. Supplier1, Supplier2).
D-23.08	to allow users to configure visibility rules on an individual line item basis for an Reverse eAuction event so that suppliers may see if they have the current lowest bid on a line item or on a given lot, but not necessarily the lowest cumulative bid for all line items.
D-23.09	to allow users to configure the Reverse eAuction event to require all potential bidders to respond with prices on individual line item or on lots.
D-23.10	to allow users to configure the preview and bidding period (start and end date/time) of an individual Reverse eAuction event and to allow modifications before or during an event.
D-23.11	to allow users to configure tiebreaker rules for an individual Reverse eAuction event.

SOW NUM	Requirement
D-23.12	to allow users to configure whether a floor and/or ceiling price is included in a Reverse eAuction event.
D-23.13	to allow suppliers to set a bid threshold to automatically update the bid to the next increment.

5.7 SECTION E: SERVICE PROCUREMENT MANAGEMENT

The GC has a significant volume of spend in Service Procurement, especially in relation to Temporary Help Services (Contingent Labour) and Professional Services. As a result, there are a number of functional requirements outlined to support this area in terms of e-Sourcing and creation of an e-Catalogue. The following are the high-level objectives of Service Procurement Requirements.

5.7.1 Catalogue

The objective of this section of requirements is to describe the configurability and management of the content in service catalogues specifically, in addition to the requirements outlined in the section D (Procurement Management). It also describes requirements related to the linking of specific resource categories to standardized resource qualifications.

5.7.2 Shopping Cart

The objective of this section is to describe the Shopping Cart requirements that are required for services catalogues, in addition to the requirements outlined in the section D (Procurement Management).

5.7.3 Ordering

The objective of this section is to describe the Ordering requirements that are required for services catalogues, in addition to the requirements outlined in the section D (Procurement Management).

5.7.4 Statement of Work (SOW) Management

The objective of this set of requirements is to ensure robust Statement of Work functionality within the EPS, specifically to allow the Government of Canada to recall, reuse and amend previous SOWs or create new ones in order to award single or multiple Contracts. The requirements in this section describe the creation of new SOWs in a variety of ways, including manually (either within or outside the system), filling out specific fields of a standardized SOW, selecting content from a SOW Builder, or by selecting and editing pre-approved SOWs from a library within the EPS.

Specifically, the e-Catalogue functionality must include the ability for GC users to create SOWs manually (e.g. free form or as an attachment); to complete SOWs using templates created within the EPS; to configure, customize and populate the SOW's template created within the EPS, and to access and re-use previously developed SOWs (from the EPS SOW Library) to create the specific SOW for their Order. Where necessary, the e-Catalogue functionality must also allow authorized GC users to amend a created SOW (e.g. to increase order quantity, change resources, etc.) in accordance with the terms and conditions of the e-Catalogue.

In addition to the requirements to support SOW for e-Catalogues, this functionality must support the SOW requirements for any Sourcing Event.

5.7.5 Resource Management – Performance Management

The objective of this section is to describe how vendor and resource performance is to be collected, tracked, and managed within the EPS for both Orders issued under e-Catalogue and Contracts issued under e-Sourcing.

5.7.6 Master Resource Record

The objective of this section is to describe the requirements for the functionality of a Master Resource Record within the EPS for both e-Sourcing and e-Catalogue. The business objectives as they relate to the requirements of this section are:

- to reduce duplication and streamline the process for managing resource data in the EPS; and
- to collect, store, and manage a variety of information regarding resources that have previously been or are currently contracted by the GC, which can be referenced by certain users at any time during and outside the ordering process.

5.7.7 Requirements

Table 100 - Service Procurement Requirements

SOW NUM	Requirement
E-01.00	**Catalogue - General** The Contractor must deliver a solution that provides the functionality:
E-01.01	to procure a variety of services (e.g. Temporary Labour, Consulting, Recurring Service, Rentals, Maintenance).
E-01.02	to capture header and line level details in the Catalogue including Work Location, Start and end date, basis of payment (e.g. time and materials, fixed price), method of payment (e.g. single, milestone, monthly), and travel and living expenses.
E-02.00	**Catalogue - Management** The Contractor must deliver a solution that provides the functionality:
E-02.01	to allow authorized administrators to create and manage configurable resource categories and subcategories (e.g. category is Project Manager, sub-category is IT or Construction) with generic descriptions of each, and attach them to more than one Method of Supply or one-off contract.
E-02.02	to allow users to create and manage resource qualification requirements using a combination of mandatory criterion and point criterion with weightings and pass marks for a specific category and sub-category in order for a supplier to demonstrate how a resource meets the applicable resource qualifications.
E-02.03	to authorized administrators to configure authorized access to view and change resource qualifications for specific resource categories or sub-categories.
E-02.04	to allow users to set fixed prices, ceiling prices, and rates for geographical areas and individual categories for all suppliers or to set individual prices for individual suppliers.

SOW NUM	Requirement
E-02.05	to allow users to configure the bidding transparency (e.g. sealed-envelope bidding) for Orders in a Catalogue that require a technical evaluation.
E-02.06	to allow authorized administrators to configure a collaboration period (e.g. interaction in the solution) between the user and Supplier(s) under a Method of Supply in accordance with the Ordering Business Rules, allowing Suppliers to submit proposals.
E-02.07	for suppliers to indicate if they have a local office in the applicable region within the Catalogue and for authorized administrators to configure when this information is displayed to a user in the ordering process.
E-02.08	for suppliers to indicate at which locations they offer specific services (e.g. what aircraft are available at an air base) within the Catalogue to assist the user in the selection of a supplier during the ordering process.
E-02.09	to allow suppliers to change their status of availability of their services, and for the solution to automatically bypass suppliers who are not available during the Ordering Business Rules process.
E-03.00	**Shopping Cart - General** The Contractor must deliver a solution that provides the functionality:
E-03.01	for suppliers to submit questions in relation to a Shopping Cart request and for the user to meta tag the question and to publish and edit the question and response in both official languages during the response period for all suppliers to view (e.g. Q/A form) without the supplier name being published.
E-03.02	for authorized administrators to view the status of the supplier's response to a specific Order (e.g. indicated no interest, evaluated but rejected, not yet invited, Order issued) within invited supplier list during the ordering process.
E-03.03	to authorized administrators to configure the evaluation status of proposed resources (e.g. viewed, under evaluation, shortlisted, accepted, rejected) and to display and configure certain notifications to be sent to suppliers regarding the respective status.
E-04.00	**Shopping Cart - Creation** The Contractor must deliver a solution that provides the functionality:
E-04.01	to inform the user of invited suppliers' preference of language for each respective Method of Supply and regional level prior to creating the Shopping Cart request.
E-04.02	to apply milestone payments based on a configured amount of the total Order value stated in the Shopping Cart request (e.g. Supplier receives $40,000 for delivering Milestone 1, and remaining $60,000 for Milestone 2).
E-05.00	**Shopping Cart - Proposal Evaluation** The Contractor must deliver a solution that provides the functionality:
E-05.01	for authorized administrators to configure whether a supplier proposal is required to be evaluated according to the resource qualification(s) listed in a SOW.
E-05.02	to notify the supplier that their proposal contains incomplete mandatory fields (e.g. has not responded to each individual qualification and/or has not attached the necessary documentation) and for the GC user to accept or reject supplier responses that are incomplete.

SOW NUM	Requirement
E-05.03	for suppliers to submit qualification details in a standard non-resume template format (e.g. grid) that responds to individual requirements of the Order/Contract.
E-05.04	for users to set up a proposal evaluation team and assign one or more members to certain criteria/areas of the proposal to be evaluated individually for the final evaluation to be completed using consensus or averaging methodology.
E-05.05	to complete an offline evaluation and import the evaluation result documents to update the status of submitted resources.
E-05.06	to evaluate the resource's qualifications against the specific category requirements (e.g. Mandatory, point-rated with weightings and with pass marks).
E-05.07	to permit the user to clarify with the supplier any aspect of their proposal that may require additional information (e.g. missing proof of certification).
E-05.08	for users to accept or reject resource proposals including explanatory comments with the functionality to set the final status.
E-06.00	**SOW Management - General** The Contractor must deliver a solution that provides the functionality:
E-06.01	for authorized administrators to configure whether the user is required to use a Standard SOW, or is required to create a new SOW.
E-06.02	to source multiple resources under one SOW with a single supplier (e.g. both Business Analyst and Project Manager from Company A).
E-06.03	to split a SOW for multiple resources into a multi-awarded supplier contract (e.g. Business Analyst from Company A and Project Manager from Company B).
E-06.04	for users to configure the applicable payment percentage that is to be attached to each milestone in the Shopping Cart request (e.g. Supplier receives 40% of payment for delivering Milestone 1, and remaining 60% for delivering Milestone 2).
E-07.00	**SOW Management - Manual Creation** The Contractor must deliver a solution that provides the functionality:
E-07.01	to allow users to create a SOW manually (e.g. outside the SOW builder, standard SOW template, and library), either by creating one within the system or importing one that was created outside the system.
E-08.00	**SOW Management - Standard SOW Creation** The Contractor must deliver a solution that provides the functionality:
E-08.01	to allow users to create and manage standard Statements of Work (SOWs) templates with configurable fields (e.g. project background, deliverable due dates) for specific categories and subcategories of a Method of Supply, which can be filled out by the user in both official languages.
E-09.00	**SOW Management - SOW Builder** The Contractor must deliver a solution that provides the functionality:
E-09.01	to create a SOW by guiding a user through a "SOW builder" in selecting sections and applicable content from a pre-approved repository (e.g. background, tasks, deliverables, constraints).
E-09.02	for users to browse, search, sort, and filter content in the SOW builder.

SOW NUM	Requirement
E-09.03	for authorized administrators to configure and manage the sections and related content in the SOW builder by central and/or distributed administrators.
E-09.04	to allow users to create a new section and applicable content to add to the specific SOW.
E-09.05	for users to add additional content to any section within the specific SOW (e.g. content not included in the SOW builder repository).
E-09.06	for users to save newly created sections in the SOW builder repository.
E-10.00	**SOW Management - SOW Library** The Contractor must deliver a solution that provides the functionality:
E-10.01	to configure and manage a library of sample SOWs by central and/or distributed administrators.
E-10.02	for users to browse, search, sort, filter, and select sample SOWs in the SOW library.
E-11.00	**SOW Management - SOW Amendments** The Contractor must deliver a solution that provides the functionality:
E-11.01	for users to amend an existing SOW at any point during the contract lifecycle (e.g. adding deliverables).
E-11.02	to redline amendments made to a SOW which will automatically be tracked in a change log, including the dates the changes were made and by which user.
E-11.03	for users to select which version of the SOW they want to compare the redlined amendments to (e.g. want to only view the redlines between versions 3 and 4 of the SOW, hiding all amendments made before this time).
E-11.04	to send SOW amendments to proceed through an approval workflow prior to being published.
E-11.05	to present an updated version of the SOW without the redline changes.
E-11.06	to manage version control of the SOW and only publish certain versions for supplier(s) to view as part of an original or amended RFx, Contract, or Order.
E-12.00	**Ordering - Management** The Contractor must deliver a solution that provides the functionality:
E-12.01	for users to create and manage Orders with a combination of time and material and deliverable-based services.
E-12.02	to allow users to configure the allocation of the limitation of expenditure for the services and any direct expenses in an Order either by group or individually within a Contract (e.g. $100,000 available for both services and Travel & Living, or $50,000 available for services and $50,000 for Travel & Living).
E-12.03	to allow users to allocate the distribution of Order award amounts in a variety of ways (e.g. at item level, at Order level, geographical region, timeframe) to track and manage the dollar amount limit available on the Order.
E-12.04	to allow users to manage and track dates for Orders for services involving multiple deliverables and/or milestones (e.g. date received, comments).
E-12.05	to allow users to configure Change Order types as either being irrevocable or requiring supplier approvals.

SOW NUM	Requirement
E-12.06	for users to initiate a replacement resource change request in accordance with the original order, provide a reason for the request (using a pre-selected list with an explanatory field), and conduct an evaluation of the proposed resource as required.
E-12.07	for users to initiate a proposed replacement resource who meets or exceeds the qualifications of the original resource on the Order.
E-12.08	for suppliers to enter and submit timesheets against Orders and for users to accept or reject them with comments and for the Supplier to resubmit after changes.
E-12.09	for users to configure optional periods, optional work, and optional quantities for their order.
E-13.00	**Resource Management - Performance Management** The Contractor must deliver a solution that provides the functionality:
E-13.01	for users to document and manage individual resource performance and to link the performance to the applicable supplier and to view the individual resource performance linked to all suppliers (e.g. John Doe worked for Company A and Company B. The user can see all of John Doe's performance. John Doe's performance is linked to the individual company he worked for.).
E-13.02	for users to configure scheduled individual resource performance reviews for the client to complete on a periodic basis (e.g. every 2 months, at end of contract only).
E-13.03	to ensure only authorized administrators as part of bidding, ordering, or the contract management process can review an individual's specific and aggregated resource performance.
E-13.04	to configure a starting performance score for suppliers without prior Government of Canada performance evaluations in a particular commodity that can be applied to the applicable Ordering Business Rules or Supplier Selection Methodology.
E-13.05	to enter, manage, and display an individual resource's performance on an Order using configurable objective and subjective criteria based on the Method of Supply.
E-14.00	**Master Resource Record** The Contractor must deliver a solution that provides the functionality:
E-14.01	to store information in a Master Resource Record that can be accessed by users at any time.
E-14.02	for authorized administrators to activate and deactivate resource profiles.
E-14.03	for authorized administrators to create and manage resources using a unique identification, regardless of the supplier organization.
E-14.04	to store resource qualifications and certificates (e.g. Diplomas, certificates, first-aid certification) including any applicable expiry dates, and notify users when expiry dates are approaching and/or require validation and/or renewals.
E-14.05	for authorized administrators to configure a workflow to validate submitted resource qualifications and certificates prior to user acceptance.

SOW NUM	Requirement
E-14.06	for suppliers to maintain their version of the proposal resource profile for a specific resource (e.g. if there is more than one supplier proposing the same resource) and update the qualifications, with the option for the user to view both the redline changes and final versions.
E-14.07	for authorized administrators to conduct and capture a project reference check to validate the accuracy of the proposed resources qualifications and experience related to that reference presented by the supplier.
E-14.08	to retrieve and provide the up-to-date information, including security level expiration date, and active status, of resources security clearance from the CISD database as well as ensuring that the supplier is holding a copy of the resources' security clearance.
E-14.09	to identify if an individual resource or supplier has previously done work for the client organization.
E-14.10	to reference information in the Master Resource Record for an initial system pre-evaluation of proposed resources against the applicable qualifications of the resource category.
E-14.11	for a suppliers' proposed resource, that has previously been evaluated and approved for a specific category/sub-category, to not require re-evaluation for a configurable period of time for the applicable category/sub-category.
E-14.12	for users to select the supplier and the applicable pre-qualified resources for a specific service category or subcategory when the resources were pre-qualified for a specific Catalogue/contract.
E-14.13	for individual organizations to create and manage configurable onboarding and offboarding activities for individual resources for a specific contract (e.g. assigning assets/inventory, issuing security IDs), with the ability to attach accompanying documentation and assign an owner to each activity.
E-14.14	to track the status of onboarding and offboarding activities and to configure dates of which to escalate non-completed activities by sending a notification to the appropriate user (e.g. the non-disclosure agreement for a specific resource has not been signed yet, marking it as incomplete).

5.8 SECTION F: FINANCIAL MANAGEMENT

5.8.1 Objectives

The overall objective of this section is to describe the requirements for the financial management functionality within the EPS, including:

- General;
- Goods Receipt Management; and
- Invoice Management.

5.8.2 General

The General subsection of these requirements must permit specific users to view, accept, and reject invoices and goods receipts, and provide users the flexibility to add comments and attachments electronically.

5.8.3 Goods Receipt Management

The Goods Receipt Management subsection is to allow for the configurability of partial and multiple receipts of Goods and Services to be handled within the EPS.

5.8.4 Invoice Management

The Invoice Management subsection includes requirements to around the receipt, management, and acceptance of invoices, while ensuring that the invoices are assigned to its corresponding Order and those elements of the invoice can be completed electronically.

5.8.5 Requirements

Table 101 - Financial Management Requirements

SOW NUM	Requirement
F-01.00	**General** The Contractor must deliver a solution that provides the functionality:
F-01.01	to allow user to reject, accept and provide comments against invoices and goods receipt as part of a two, three or four way matching.
F-01.02	to allow a user to add attachments (e.g. Expense receipt) to an invoice.
F-01.03	to browse, search, sort and filter invoice and goods receipt details.
F-01.04	to provide ongoing status updates to the end user upon receipt of Invoice until completion of the Order.
F-01.05	to configure either percentage and dollar amount tolerance levels between item quantities, price elements on the contracts and/or Orders, Invoices and Goods Receipt to support two, three and four way matching and perform specific actions (e.g. Despatch and receipt advice, Invoice and actual goods received).
F-01.06	to send the calculated discount adjustment and the early payment date information to the end user which will be tied to two/three/four way matches.
F-01.07	to configure notifications for users (e.g. Status of Invoice/good receipt, credit memo, payment refusal, Order details, status notifications, back order).
F-01.08	to configure a notification period based on contractual payment terms (e.g. payment period).
F-01.09	to integrate scanning devices/software to input goods receipt information into the system and connect to the applicable Order (e.g. warehouse loading dock receipt process).
F-02.00	**Goods Receipt Mgmt** The Contractor must deliver a solution that provides the functionality:
F-02.01	to allow partial receipts and multiple receipts for single or multiple Order items.

SOW NUM	Requirement
F-02.02	to configure workflows to allow goods receipt approval on behalf of multiple or single cost centers.
F-02.03	for an authorized administrator to configure the movement types for the receipt of goods or services in accordance with departmental financial materiel management system (e.g. goods received, damaged).
F-02.04	to allow a user to reject a goods receipt.
F-03.00	**Invoice Mgmt** The Contractor must deliver a solution that provides the functionality:
F-03.01	to allow suppliers to view rejected and/or accepted invoice comments and resubmit rejected invoices.
F-03.02	to track and record the return of goods to a supplier (e.g. Damaged goods, incorrect quantity/quality, incorrect goods).
F-03.03	to apply Credit notes to any invoice for a supplier.
F-03.04	to configure and compare the Invoice, Order and receipt details and perform quality control to determine manual and automatic actions required (e.g. Two, three, and four way matches).
F-03.05	to submit invoices in the currency of the contract.
F-03.06	to allow suppliers to submit invoices and credit memos in multiple currencies in at least the following methods: a) Manual input: Data is inputted into a standard form with required and optional fields. b) Uploaded file: Data are uploaded in a structured file format (e.g. XML, UBL). c) Machine-to-machine: Suppliers can set their financial systems to automatically and directly transmit information using EDI or web services.
F-03.07	to allow supplier to submit an invoice based on Electronic Document Interface (e.g. Goods receipt, trade discounts) and via web services.
F-03.08	to configure a Self-invoice (prefix/suffix) number that can be tied to the Order number.
F-03.09	to generate an Invoice/goods receipt with the Order details (e.g. flip an Order into an Invoice).
F-03.10	to prevent a supplier from invoicing line items, depending on the basis of payment (e.g. milestone, lump sum) for more than a configurable percentage of their estimated cost.
F-03.11	for suppliers can override dynamic discounting preference (e.g. discount terms) for a specific invoice.
F-03.12	to automatically apply the trade discount terms for all Invoices against the applicable Contract/Order.
F-03.13	to offer suppliers the option of receiving early payment through dynamic discounting.
F-03.14	to allow a user to configure a manual Invoice template that will contain Order details (e.g. trade discounts).

SOW NUM	Requirement
F-03.15	to send line level Invoice and Goods Receipt information to the departmental financial materiel management system in order to initiate the payment.

5.9 SECTION G: BUSINESS INTELLIGENCE

5.9.1 Overview

Business intelligence (BI) is a technology-driven process for analyzing data and presenting reportable information to help executives, managers and other end users make more informed business decisions. This business area encompasses a variety of tools, applications and methodologies that enable organizations to collect data from internal systems and external sources, prepare it for analysis, develop and run queries against the data, and create reports, dashboards and data visualizations to make the analytical results available to decision makers as well as operational workers.

This business area is divided into 4 sub-sections:

- G-01 General (configuration, search, format and template functions)
- G-02 Reporting (functions to generate various types of reports)
- G-03 Analytics (various data analysis, variance analysis and calculation functions)
- G-04 Report and Analytics Dashboard (creation and configuration of interactive dashboards).

5.9.2 Requirements

Table 102 - Business Intelligence Requirement

SOW NUM	Requirement
G-01.00	**General** The Contractor must deliver a solution that provides the functionality:
G-01.01	to configure, add, delete and modify fields in reports.
G-01.02	to search, filter, group, view and report by various parameters including, but not limited to: a. all user entered and defined data fields (e.g. contract fields, attributes, metadata, and geographic areas); b. all system captured and stored data; c. all aspects of procurement process (e.g. from Requisition to Payment); and d. all procurement hierarchies, dimensions, measures and performance metrics/KPIs (e.g. commodity, supplier, time, dollars of sales, number of hours/days, number of past-due accounts).
G-01.03	to create and display highly formatted, print-ready and interactive reports in various formats including, but not limited to the following: a. tabular; b. columnar;

SOW NUM	Requirement
	c. cross tab or pivoted; and d. banded.
G-01.04	to deliver and support preconfigured, formatted, print-ready business reports with or without parameters that can publish and graphically depict data and measures from various procurement business objects, including, but not limited to summarized and detailed reports on: a. purchasing orders; b. requisitions; c. catalogue items; d. contracts; e. sourcing projects; and f. suppliers.
G-01.05	for users to discover, view, analyze, report and compare real-time data with historical data for all procurement business objects.
G-01.06	for users to schedule and automatically generate, print and distribute reports on a predetermined basis defined by the user.
G-01.07	to allow authorized administrators to create and configure report distribution list and automatically generate and distribute reports to addresses and locations specified on the list including, but not limited to: a. email notification delivery; and b. file share delivery.
G-01.08	for users to subscribe and unsubscribe to an automatic report distribution list.
G-01.09	for users to export standard pre-packaged and user defined reports to various file formats and software such as, but not limited to: a. MS Excel/MS Word; b. 3rd party BI software packages; c. CSV file; d. XML file; and e. PDF.
G-01.10	to configure report parameters and performance metrics for reporting on various procurement activities, including, but not limited to: a. performance trends (e.g. supplier, quality, time, contract); b. contract metrics (e.g. spend %, leakage %); c. changes in Contracts and Orders (dollar amount, quantities); d. roll-up summary and snapshots of data at any given point in time; e. pre-defined or user defined Key Performance Indicators (KPI) thresholds; and f. key milestones and deliverables.
G-01.11	for authorized administrators to configure reports access rights and grant or restrict access and view of reports and data in line with user's access privileges.

SOW NUM	Requirement
G-01.12	for authorized administrators to create, manage and publish standard report templates and make them available to other users.
G-02.00	**Reporting** The Contractor must deliver a solution that provides the functionality:
G-02.01	for users to generate operational category specific reports such as, but not limited to: a. requisition related operational reports; b. bid evaluation related operational reports; c. contract related operational reports; d. purchasing order related report; e. operational reports that can show various procurement summary information; and f. operational reports for all workload activities.
G-02.02	for users to generate drill-through reports to view information at a specific level, and drill to other levels of information on a user-selected value.
G-02.03	for users to generate detailed and summary end-to-end reports that present each step of procurement processes and everything that happens from requisition to payment.
G-02.04	for users to generate static "point in time" reports and save them for future use.
G-02.05	to enable users to build their own custom queries and reports using the solution's ad-hoc query and reporting tool that has a reusable semantic layer with familiar and common business terms that allows user, without being technically savvy, to: a. navigate available data sources; b. access predefined metrics; c. navigate hierarchies.
G-02.06	to generate report on the status and data matrices of procurement opportunities such as, but not limited to: a. number of procurement opportunities and their status; b. processing time (e.g. by Supplier, By Client etc..); c. number of transactions (e.g. user actions, number of purchases etc.); and d. approval stage and status.
G-02.07	to generate and create reports that summarize and calculate various amounts and volumes with totals and sub totals.
G-02.08	to generate reports that can rank suppliers and show trends in supplier performance over time based on various collected data, such as, but not limited to: a. quality; b. supplier's delivery performance; and c. service performance.
G-02.09	to generate spend reports that can show various summary and detail reports such as, but not limited to: a. potential savings; b. year over year Spend by commodity categories and supplier;

SOW NUM	Requirement
	c. cumulative Spend by purchase order and by invoices; and d. Spend reports for supply arrangements and standing offers by various parameters (e.g. by supplier, region, etc.).
G-02.10	to generate reports on user and group access to individual solution components and objects, including but not restricted to: a. full and partial access to procurement file(s); b. user and group functionality rights, privileges and restrictions for assigned components; c. user and group information access rights, privileges and restrictions; and d. user and group access to meta-data properties.
G-03.00	**Analytics** The Contractor must deliver a solution that provides the functionality:
G-03.01	for users to conduct various types of data analysis such as, but not limited to: a. trend and performance analysis and monitoring; b. Supplier Fragmentation Analysis; c. Forecasting; d. Time Series Analysis; e. What if Scenarios; f. Goal seeking and optimization analysis; g. Regression Analysis; h. Statistical / Financial Functions and Formulas; and i. Segmentation.
G-03.02	for users to perform analysis, multidimensional calculations and aggregation of the data and view up to date information for all aspects of a procurement including, but not limited to: a. calculated savings and expenditures by various factors; b. purchases by various factors; c. usage of selected clauses from the clause library; and d. award of contracts by various factors.
G-03.03	to allow for variance analysis in dollars, percentages, time (i.e. delta between any sums, variance based on time such as hours/days and/or dates).
G-03.04	to support line item level Business Intelligence and detailed analysis (i.e. how many units of an item were purchased, by who, from whom, for how much, and under what contract).
G-03.05	to analyse and calculate the growth of processed transactions within a specific time period by various parameters (e.g. by supplier, by client).
G-03.06	to aggregate fact table measurement data by key data elements such as, but not limited to supplier, amount, accounting.
G-03.07	to analyse data by various factors, including, but not limited to, item, region, supplier, client, socio-economic issue.

SOW NUM	Requirement
G-03.08	to support analysis on user defined additional configurable fields from all relevant procurement related fact tables (e.g. Requisitions, POs, Contracts, Invoices).
G-03.09	to allow flexible grouping of procurement data elements across multiple dimensions such as, but not limited to, suppliers, products, services, contracts, location and time.
G-03.10	to measure and analyse contract forecasted and actual spend and implemented savings by various factors, such as, but not limited to business unit and location.
G-04.00	**Reporting and Analytic Dashboard** The Contractor must deliver a solution that provides the functionality:
G-04.01	to enable and support a broad range of Business Intelligence data visualization tools including, but not limited to: a. display of multiple diverse objects on a page like table, picture and text; b. various types of Charts (e.g. Bar, scatter, combination, pivot, line, radar, area, high-low, stacked bar); c. various types of graphs with target indicators (e.g. Line, bullet, bubble) d. meters and gauges; and e. 2D and 3D charts and graphs.
G-04.02	for users to Configure and create highly interactive reporting and analytic dashboards and define metrics and data content with visual exploration and embedded advanced analytics.
G-04.03	for users to configure and create reporting and analytical dashboards with operational and strategic information that allow things such as, but not limited to: a. production, distribution and printing of reports and widgets b. configuration of parameters, filters and prompts c. guided dashboard navigation
G-04.04	for users to configure and generate a dashboard report that shows all sourcing initiatives in progress, their status and timelines.
G-04.05	for users to configure and generate custom data views on reporting and analytic dashboards and reporting pages.
G-04.06	for users to seamlessly move from reporting and analytic dashboard to all relevant procurement modules and spend management applications.
G-04.07	for users to join multiple fact tables in a single view (e.g. PO and Invoice).

5.10 SECTION H: SUPPLIER RELATIONSHIP MANAGEMENT

5.10.1 Overview

Supplier Relationship Management (SRM) includes management of Supplier registration, communications with one (1) or more Suppliers, and enabling the capture, tracking and measurement of performance including evaluation tools such as client surveys, and the ability to take action with respect to a Supplier's registration status based on those performance evaluations.

This business area provides end-to-end supplier lifecycle supporting capability for lowering costs, reducing risk, and facilitating more effective relationships with suppliers. The SRM is a single, centralized digital supplier repository including: a credentials screening function through a supplier portal that enables suppliers to enter information on pre-established forms and/or upload required procurement related documents. Business functions of the SRM include:

Onboarding: The establishment of trusted relationships with new suppliers, through the secure self-service management of supplier product lists, price lists, and catalogues, while maintaining the ability to track supplier performance and report on and renew supplier qualifications and certifications;

Supplier repository: Automatically aggregates all supplier data from internal and external sources and allows for each supplier file to reflect all supplier relevant information such as vendor performance, financial risk, ecological profile, pending litigation, contracts etc.

Supplier risk management: Encompasses all tools used to model, map and track the chance of undesired events associated with suppliers which may have a detrimental effect on purchasing operations and outcomes. It includes the ability to monitor contract compliance, identify risk sources (frameworks for applying a systematic approach to risk management), develop risk indicators and subsequently assist in managing and monitoring operational supply risk, and implementing vendor corrective action as required.

Supplier performance and credentials: Supplier Performance management ensures the supplier's performance meets the expectations defined in the contract. It includes the management of actual performance, identification of performance gaps and agreement of actions to achieve desired performance levels. Supplier credentials provide for the management of a supplier's certifications, (legal documents, quality assessments, security clearances, integrity certifications, etc.) allowing for validity period monitoring and automatic follow up of missing or expiring documents.

SRM supports supplier's self-registration. Information provided by the suppliers must comply with Industry Canada Legal Name and Business sector information as well as Revenue Legal Name and Business Number and business sector's prerequisites such as licenses, certifications and security clearance, among others, to be validated in EPS. Information captured is used during various steps of the Contract Lifecycle Management for example, during bid evaluation, issuance of a standing offer or termination of a contract among others.

This business area is divided into 5 sections:

- **H-1 Supplier Profile Management** (functions to support supplier self-registration, using predetermined and secured access permissions)
- **H-2 Performance** (functions to assess vendors' performance and allow users for example to view, analyse, compare, administer and interpret performance results)
- **H-3 Evaluation Tools** (functions to run multiple types of survey and allow users for example to assemble, reuse, validate, conduct, administer and interpret surveys)
- **H-4 Search Functions** (functions to the system to support searching capabilities for users and suppliers through robust search engine capabilities using, for example, key word or other related data.)

- **H-5 Notification** (functions to notify users and suppliers, in multiple ways, for example about rights pending, scheduled events, reminders for action and escalation or for validation of actions.)

5.10.2 Requirements

Table 103 - Supplier Relationship Management Requirements

SOW NUM	Requirement
H-01.00	**Supplier Profile Management** The Contractor must deliver a solution that provides the functionality:
H-01.01	for authorized administrators to configure standard supplier on-boarding process which includes, but is not limited to: a. approvals and tasks when supplier registers; b. recurring tasks; and c. variations in registration process (e.g. by commodity, by region, by supplier status).
H-01.02	for authorized administrators to create and configure an intelligent supplier self registration form with optional, mandatory and editable fields that will prompt the supplier for further information and documents based on combinations of configurable business rules and provided information.
H-01.03	for authorized administrators to configure supplier profile questions in order to collect supplier credentials and certification and store them under suppliers profile at various times, including, but not limited to: a. when supplier registers into the system; and b. when supplier completes and submits a response to an RFx.
H-01.04	for authorized administrators to configure the workflow process for the approval of supplier registration and submitted credentials and certifications.
H-01.05	for authorized administrators to configure business rules and set parameters for supplier's activation/deactivation including but not limited to: a. authorized user turns on/off functionality to activate/deactivate supplier; and b. system automatically activates/deactivates supplier's accounts parameters.
H-01.06	to support Parent/Child supplier organizational hierarchies and tree like classification and management of suppliers.
H-01.07	to support storage, maintenance and retrieval of all previously submitted versions of documents from the supplier's profile including, but not limited to: a. credentials; b. certifications; c. insurance policies; and d. financial statements.
H-01.08	to ensure completeness of supplier's data and data quality including, but not limited to: a. preventing duplication of suppliers; and

SOW NUM	Requirement
	b. raising the alerts on suppliers with missing, incomplete as well as mismatching data in their profile
H-01.09	to utilize a single and unique supplier ID number across the entire procurement process and allow traceability of a supplier throughout the process.
H-01.10	to enable supplier to set up their interests for a single and multiple commodities (e.g. by commodity code, by service offering, by region).
H-01.11	for suppliers to manage and maintain information pertaining to, but not limited to, their licenses, security clearance, qualifications and certifications as a part of supplier profile including, but not limited to: a. import and attach electronics copies of their qualifications certifications in multiple formats including, but not limited to .PDF, .PPT, .BMP, .GIF, .JPEG, .JPG; and b. enter and update validity period of qualifications and certifications (e.g. expiry dates).
H-01.12	for authorized administrators to validate and approve information and certificates provided by the supplier, including, but not limited to: a. professional certifications; b. insurance policies; c. security clearances; and d. financial statements.
H-01.13	to define, associate and maintain supplier registration with geospatial and locational information including, but not limited to: a. geographical radius and location; b. geographical zones; and c. regions.
H-01.14	to pull information from supplier's response to a sourcing event into its supplier profile.
H-01.15	to support supplier self registration through a standardized and intuitive registration process that allows Canadian and International suppliers to acquire a single and unique supplier ID (i.e. Procurement Business Number) in order to register in to the system.
H-01.16	to pull, share and validate supplier information and data in real-time from and against equivalent information in third party content providers and systems (e.g. CRA, SAP) and ensure integrity of the data between different systems including, but not limited to Legal Name and Procurement Business Number.
H-01.17	to pre-populate supplier registration form with information and data from other systems and enable a supplier to maintain their own information including, but not limited to: a. name, address, contact information; b. aboriginal owned; c. controlled goods registration; d. financial Statements;

SOW NUM	Requirement
	e. direct deposit payment information; f. Ghost Card credit information; and g. special characteristics of their business.
H-01.18	to support registration of multiple suppliers jointly as a single supplier (e.g. Joint Ventures) including, but not limited to: a. create Joint Venture account; b. provide and assign a unique business number to the Joint Venture; c. ensure that the Joint Venture legal name shows the names of all companies participating in the Joint Venture within the solution; d. Ensure that that the Joint Venture legal name can be created as a distinct from the names of the parties to the JV; e. Allow JV supplier to identify business characteristics, such as: name, location, delivery address, billing address, ghost credit card information, etc.; f. Ability to allow user to link all of JV information to each of its individual members; g. Pre-populate information about each member of the Joint Venture from their existing profile; h. Allow user to remove one or more members of JV; i. Allow JV to remain active even when one or more members of JV are removed; and j. Deactivate Joint Venture (e.g. Joint Venture dissolves).
H-02.00	**Performance** The Contractor must deliver a solution that provides the functionality:
H-02.01	for a Contracting Officer to record and monitor supplier performance throughout the contract lifecycle.
H-02.02	for a Contracting Officer to add notes on supplier performance before closing Contract, Order, Framework Agreement.
H-02.03	to track, measure and report on the performance progress of suppliers and use a performance review as an input into future solicitations and contracts with the supplier.
H-02.04	for a Contracting Officer to access supplier performance evaluation history information and data at any time including but not limited to: a. during the RFx evaluation; b. during Contract Management; and c. during procurement File Close-Out.
H-02.05	to maintain a repository of surveys and scorecards which is accessible only through Role Based Access and organized in a number of ways, including, but not limited to: a. contracts; b. framework agreements; and c. suppliers.

SOW NUM	Requirement
H-02.06	for a Contracting Officer to create configurable surveys and scorecards to assess and report on supplier performance including, but not limited to performance on: a. orders; b. framework agreements; c. contracts; and d. overall performance.
H-02.07	for authorized administrators to configure and create separate survey versions specific to a particular subject including, but not limited to: a. geographic location; b. procurement; and c. stakeholder.
H-02.08	for authorized administrators to configure and schedule survey.
H-02.09	for users to define, update and maintain Key Performance Indicators as part of performance management process.
H-02.10	to define maximum and target points for each Key Performance Indicator for a supplier or category.
H-02.11	to raise a flag and notify a configurable list of users when Key Performance Indicator score is below established targets.
H-02.12	to allow drill-down and roll-up up on Key Performance Indicators to evaluate results on a more detailed level.
H-02.13	to map survey questions to specific Key Performance Indicators and automatically pull in data from survey responses to pre-populate a scorecard.
H-02.14	to consolidate and merge results from multiple surveys into a single scorecard.
H-02.15	to route scorecards for review by identified users.
H-02.16	for users to collaborate with suppliers on scorecard results and associated action items.
H-02.17	for suppliers to have 'view-only' access to their scorecards and survey results.
H-02.18	to pull in qualitative and quantitative data from both third party sources and from within the solution as part of scorecard generation.
H-02.19	to support various scorecard features, including, but not limited to: a. graphing of scorecard results; b. generating scorecards for different level of performance (e.g. performance is above, at-risk or below targets); and c. rank suppliers for specific commodities by weighing scores on score carding (e.g. highest and lowest).
H-02.20	for authorized administrators to configure and maintain process to debar a supplier that includes but is not limited to: a. configuration of workflow to govern (e.g. set, remove) debarment and handle exceptions; b. configuration of alerts and triggers that prompts users of debarred suppliers;

SOW NUM	Requirement
	c. configuration of business rules that would prevent a user from issuing contracts, orders, or framework agreements to debarred supplier; d. configuration of business rules with decision points that can prevent or allow debarred suppliers to bid on competitive procurements; and e. configuration of business rules with a decision points that would make debarred supplier's catalogues unavailable to users.
H-02.21	for a Contracting Officer to debar a supplier through workflow managed process including, but not limited to debarment: a. across-the-board (affecting all aspects of the supplier's operations); b. for a specific period of time; c. for a specific geographic region ; d. for a specific commodity; and e. for a specific type of contract or framework agreement.
H-03.00	**Evaluation Tools** The Contractor must deliver a solution that provides the functionality:
H-03.01	for authorized administrators to distribute a survey to be completed by the respondents.
H-03.02	for authorized administrators to distribute surveys.
H-03.03	for authorized administrators to copy previously created surveys for re-use.
H-03.04	to allow survey creator/respondents to save partially built/completed surveys as drafts to be completed at some future point in time.
H-03.05	to allow survey creator to identify and select target survey respondents based on various parameters, including, but not limited to: a. their geographic location; and b. commodity.
H-03.06	to allow survey creator and respondents to add attachments to survey with no limit on the number or size of the attachments.
H-03.07	to distribute and track who responds to surveys with time and date stamp of response.
H-03.08	to integrate survey distribution and approval with workflow including but not limited to: a. route the survey to respondents and approvers; and b. approve posting of survey results to a scorecard.
H-04.00	**Supplier Search Function** The Contractor must deliver a solution that provides the functionality:
H-04.01	to provide robust search, browse, sort and filter capabilities including, but not limited to: a. any data field within the supplier library;

SOW NUM	Requirement
	b. any data field within the survey and scorecard library; and c. any data field within the performance evaluations.
H-04.02	to enable authorized administrators to perform faceted searches to find and view suppliers and suppliers' information including, but not limited to: a. supplier data; b. contract history; c. contact information; d. qualifications; e. certifications; and f. security information.
H-04.03	to make all data within supplier repository and performance management tool searchable and allow user to save supplier and performance management related searches (e.g. Favorite Searches).
H-05.00	**Notification** The Contractor must deliver a solution that provides the functionality:
H-05.01	to allow configuration by authorized administrators of various notification features for all activities in Supplier Relationship Management module such as, but not limited to: a. reminders that can be sent to survey participants; b. email messages as part of survey; c. scheduling of automatic events, triggers and alerts; and d. allow users to turn on/off automatic notification functionality.
H-05.02	to track and automatically notify Contracting Officer and Supplier about need for regular update and renewal of supplier's profile information including but not limited to: a. qualifications and certifications renewal due; b. security clearance information; and c. Supplier's status (active or inactive based on a set of configurable rules).
H-05.03	to track and notify authorized administrators throughout the procurement process when and if supplier's performance status is updated and changed within SRM such as, but not limited to: a. proposed winning supplier had performance issues on previous and /or current contract(s); b. supplier is debarred; and c. supplier is suspended.
H-05.04	to allow for mass notification to suppliers of announcements, changes to ongoing sourcing events or other communications.
H-05.05	for users to schedule activities and tasks associated with a supplier and notify users when tasks are scheduled to occur (e.g. a performance meeting).

5.11 SECTION I: DATA AND INFORMATION MANAGEMENT

5.11.1 Objective

The objective of this section is to describe the requirements for Data and Information Management within the overall scope of the EPS to ensure that:

- Information needs are met from different perspectives: GC Procurement policies, processes and regulations; suppliers' business needs; buyers from GC departments and agencies; stakeholders and partners.
- Information reaches high quality standards and retains its business value over its lifetime.
- Information is seamlessly flowing between various systems and databases.
- Procurement master data (classifications, vendor) is constantly evolving through manual and automated processes such as reviews, adjustment and enrichment.
- Data assets are preserved from system failures and recovery mechanisms are agreed upon, planned and implemented.
- Public information is available and shared with partners on a continuous basis (Open data).
- Opportunities are present to expand the database architecture in order to respond to changes in regulations and business needs.

In summary, the proposed data management component of the service must be robust, comprehensive, and based on commercially available, off-the-shelf data management technologies.

5.11.2 Requirements

Table 104 - Data and Information Management Requirements

SOW NUM	Requirement
I-01.00	**Notification** The Contractor must deliver a solution that provides the functionality:
I-01.01	to configure the overall data architecture and data model in accordance with approved GC enterprise architecture.
I-01.02	for the extension of the data model (e.g. add custom fields to existing tables, add custom).
I-02.00	**Database Operations Management** The Contractor must deliver a solution that provides the functionality:
I-02.01	to support the creation and exchange of all open dataset file formats including but not limited to CSV, XML, JSON.
I-02.02	to import electronic records/data directly from an external source using standard file formats including but not limited to CSV, XML, JSON.

SOW NUM	Requirement
I-02.03	to export electronic records/data to external systems using standard file formats including but not limited to CSV, XML.
I-02.04	to configure and manage regular (scheduled) and ad-hoc import/export processes using a configurable set of search criteria, fields, data formats, grouping and sorting options.
I-02.05	to configure, schedule and track data operations such as but not limited to: extracts (exporting), creation of data sets (Open Data), feeding of target data stores (OLTP, OLAP, SOA), web/online publishing (e.g. HTML/RSS-XML Feeds), system/user reports and queries.
I-03.00	**Data Quality Management** The Contractor must deliver a solution that provides the functionality:
I-03.01	to automatically monitor the quality of information (transactional and master data repositories) by evaluating the following dimensions: completeness, conformity, consistency, accuracy, duplication and integrity.
I-03.02	to measure and assess data quality by applying system and user-configurable scenarios, business-system rules and schedules, in various situations such as: • upload of new catalog items; • import of updated/new classification code schemes; • data synchronisation checks between EPS and SAP; and • transactional and master data scheduled verifications.
I-03.03	to prepare and disseminate the results of data quality verifications to authorised users in summarized or detailed forms.
I-03.04	to send notifications (e.g. Email, SMS) while assigning different levels of priority to them (e.g. Normal, urgent, critical) when potential rule-based data quality issues are detected.
I-03.05	to automatically suggest changes to transactional or master data record or group of records, to obtain confirmation from authorized administrators before applying changes and to run changes in unit or in batch as instructed by the system administrator. Changes may cover actions such as cleansing, standardisation, profiling (e.g. capture of metadata from data analysis), merging of related records or data enrichment tasks, e.g.: aggregating, cleansing, enriching and categorizing spend data across various data sources (general ledger, Enterprise Resource Planning -ERP systems, EPS, and payment).
I-03.06	to automate changes to records or group of records based on a variety of rules, such as industry and international standards, GC-EPS or departmental/agency standards and business rules, knowledge bases of values and patterns, domain restrictions, integrity constraints or other GC business rules that define sufficient data quality for the organization.
I-04.00	**Reference & Master Data Management** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
I-04.01	to create and manage manually and automatically master data as per recognized and approved industry and Government of Canada standards and specifications such as: United Nations Standard Products and Services Code® (UNSPSC®), Guideline on Common Financial Management Business Process.
I-04.02	for authorized administrators to create, configure and manage master data such as Material Master Record and Customer Vendor Master Record.
I-04.03	to process spend classification based on a number of different data elements, in a configurable precedence order, such as, but not limited, to: • supplier information; • client specific data (e.g. GL Codes, item description); • industry and customer defined product codes (e.g. UNSPC, GSIN).
I-04.04	to offer supplier data enrichment capabilities regarding data elements such as; • parent/child relationships; • Standard Industrial Codes (SIC).
I-04.05	to ensure consistent classification of similar items from different data sources using automatic and rule-based classification.
I-04.06	to allow record, and where applicable group of records, to be classified in accordance with the organisation's records classification scheme.
I-04.07	to support close linkage and interaction between records classification and other records management processes, such as capture, access and security, disposition, searching and retrieval, and reporting.
I-05.00	**Data Warehousing and Business Intelligence Management** The Contractor must deliver a solution that provides the functionality:
I-05.01	to deliver, enable and support integrated Data warehouse/On-line Analytical Processing (OLAP) capability for business intelligence (BI) and reporting, supporting analytical operations such as consolidation (roll-up), drill-down, and slicing and dicing.
I-06.00	**Document, Record & Content Management** The Contractor must deliver a solution that provides the functionality:
I-06.01	for the creation and management of document templates (e.g. procurement checklists, forms, worksheets) that may contain text, format features and fillable form elements such as: text input fields, checkboxes, drop down lists, data tables, tables.
I-06.02	for the creation of new documents through various mechanisms, such as: • using a blank or pre-defined template; • importing (upload) an existing document; • cloning an existing document as a new one; and • preparing a new composite document from a number of individual documents.
I-06.03	for metadata information to be captured during the creation of document or extracted from existing documents.
I-06.04	for new and existing document to be stored in pre-defined section of existing taxonomies (e.g. folder structure) as determined by the user.

SOW NUM	Requirement
I-06.05	for the management of documents (e.g. modify, remove, move from one taxonomy to another).
I-06.06	to map and link documents using different topologies (e.g.: one-to-many, many-to-many relationship, cross-references) as defined by users.
I-06.07	for the creation and management of bookmarks to link to favorite documents or section of documents.
I-06.08	for the validation of text fields using editing tools such as autocorrect, spellchecker and thesaurus for the appropriate official language.
I-06.09	to configure and manage the publishing workflow of procurement files and track the lifecycle of each file through its different disposition stages (e.g. draft, approved, published, archived, marked for deletion and deleted).
I-06.10	to enable and configure an integrated built-in versioning tool for individual or group of records, including features such as: configuration of version numbering, creation of minor or major versions of a document, ability to revert a document to a previous revision.
I-06.11	to enable and configure real-time collaboration on a procurement file and associated documents using features such as document versioning, document locking or conflict resolution in multiuser environments.
I-06.12	for the configuration, execution and tracking of record imports from external source.
I-06.13	to maintain the relationship between multi-component electronic records (e.g. database records, file attachments, data feeds) using various mechanisms such as metadata.
I-06.14	for the content of electronic messages to be imported from an authorized administrator's corporate email client.
I-06.15	to capture all user documents, information, and records and retain them in the system.
I-06.16	to configure the naming of electronic records through manual (user input) and automated processes.
I-06.17	for the tracking of all disposition actions carried out on electronic records (migration, import, export).
I-06.18	to report the details and outcome of any migration process to ensure the integrity of electronic records.
I-06.19	for the creation and management of disposition classes that would define: • retention periods to set how long individual or group of records must be maintained; disposition actions (e.g. review, export, transfer, archiving, destruction) to prescribe the fate of records; and • tracking of disposition actions.
I-06.20	for disposition classes to be systematically applied to existing, received or newly created records and associated metadata, and where applicable group of records.

SOW NUM	Requirement
I-06.21	to notify authorized administrator on a regular basis of all disposition actions due to occur in a specified period of time.
I-06.22	to make the entire content of a record or group of records available to reviewers, subject to applicable access restrictions.
I-07.00	**Metadata Management and Taxonomy** The Contractor must deliver a solution that provides the functionality:
I-07.01	for authorized administrators to create and manage taxonomies of different types (e.g. lists, synonyms, hierarchies (e.g. GSIN, UNSPSC), faceted navigation and thesaurus, Ontologies), such as: • to map together different taxonomies which can be defined and managed in a hierarchical fashion (e.g. Federal Stock Class, North American Free Trade Agreement (NAFTA), North Atlantic Treaty Organization (NATO), UNSPSC Coding, and Construction Specifications Institute (CSI)); • to define a hierarchy of related web pages within a section of the portal; and • to link documents of the same procurement project (e.g., requisitions, requests, bids, bid evaluations) into a tree structure.
I-07.02	for the import and export of taxonomy structure and terms using standard formats (e.g. CSV, XML).
I-07.03	for authorized administrators to create and manage metadata registries in order to store semantic and system-specific constraints about data elements such as: individual field, database table and views, schema definition of xml files used for import or export purposes (e.g. Open Data), procurement file (parts or complete document) , fixed records (e.g. PDF document) or web feeds.
I-07.04	for authorized administrators to expand the definition of data elements in the various metadata registries by adding and configuring custom data attributes (e.g. security, rights and public availability properties).
I-07.05	for authorized administrators to define rules on how metadata is captured for each instances of a record, such as: manual keying, dropdown menu feeding from taxonomies or database content, auto-complete.
I-07.06	to automatically capture metadata acquired directly from an authoring application, an operating system, an electronic records management system or generated by EPS itself.
I-07.07	to configure and restrict the ability to amend record metadata during the lifecycle of record based on business rules defined by GC.
I-07.08	for authorised users to amend, over-ride or expand metadata inherited by records and, where applicable, group of records.
I-07.09	for the capture of metadata entered manually by an authorized administrator.
I-07.10	to enable user-defined metadata fields for the entry of descriptive information about the record or, where applicable, aggregations of records.
I-07.11	for the configuration of system rules for the assignment of metadata on capture of a record, or group of records using features such as auto-classification or data tagging.

SOW NUM	Requirement
I-07.12	to support the configuration and creation of metadata elements for each record or component of a record.
I-07.13	to notify content owners of missing metadata in newly or updated documents.

5.12 SECTION J: USER MANAGEMENT

5.12.1 Introduction

The GC is a very complex organizational environment, and this organizational complexity will necessarily carry over to the nature of users within the EPS.

EPS users come from various departments. These departments have individual hierarchies of varying shapes and sizes that will need to be accurately captured within the solution. From there, users must be able to have varying delegations of authority on both a specific and general basis, requiring that the solution allow and support this function.

Also of great importance is the GC's specific need for user credential validation. This must include the use of the Government of Canada "MyKEY" for logging in to the solution.

5.12.2 Objective

The objective of the User Management section J is to describe the requirements of the User Management within the overall scope of the EPS to ensure that the proposed user management component of the EPS is robust, comprehensive, and based on functionality that is contained within commercially available, off-the-shelf enterprise technology.

5.12.3 User Management Requirements and Deliverables

The User Management section J includes roles/groups requirements, registration requirements, profiles/accounts requirements, and login requirements. The main deliverables include:

5.12.3.1 Roles/Groups

The Contractor must feature the capability to assign groups (likely consisting of types and roles) to users. This capability will need to include the ability to configure permissions and access rights according to group, as well as other more particular functions. The Contractor must have the functionality to provide a variety of user types, including, but not limited to the following: Supplier user and end user and to provide a variety of roles for users, including, but not limited to the following: Procurement Officer, Reviewer, Trainer, and "unspecified" EPS User (with full access rights and privileges).

5.12.3.2 Registration

The Contractor must provide specific features to ensure a complete and accurate registration process for users. This includes the management of user accounts, the creation of user profiles, the imposition of user account set-up prior to final registration, and the use of information stored in an electronic credential key.

5.12.3.3 Profiles/Accounts

The Contractor must provide extensive functionality around the user profiles in the EPS. This includes a number of requirements around account management, as well as being able to search through user profiles.

5.12.3.4 Login

The Contractor must allow for authentication of the user at login through the use of an electronic credential key.

5.12.4 Sample Personas and User Segmentation

Table 105 - User Personas Drive Permission and Access Requirements

	Project Team	PWGSC Acquisitions Branch			Regional Acquisition Branches	Industry	Departments and Agencies
	EPS Admin	Procurement Specialist	Vendor Manager	Sourcing Manager			
E-Catalogs	A	RW	RW	RW			
Contract Management Solution	A	R	RW	RW			
Supplier Relationship Management	A	R	RW	RW			
Sourcing Management	A	RW	RW	RW			
Procurement Management	A	RW	RW	RW			
Business Intelligence	A	R	R	R			

Table 106 - User Permissions Legend

Permission	Description
A	Administrator permissions
RW	Read-write permissions
R	Read-only permissions

Table 107 - User Permissions Key Terms Definitions

Term	Definition
Procurement Professionals	Supply professionals within the Acquisitions Program
Industry	All suppliers providing goods and services to the Government of Canada
Departments and Agencies	End Users accessing procurement information and services

The user “personas” Section 5.12.4 are for the purpose of example only, and are referred to as roles in Section 5.12.5.

5.12.5 Requirements

Table 108 - User Management Requirements

SOW NUM	Requirement
J-01.00	**User Management - Roles / Group** The Contractor must deliver a solution that provides the functionality:
J-01.01	to provide role-based access control that defines the rights of users, as well as the functionality they can use in the solution.
J-01.02	for authorized administrators to set and administer tiered levels of access rights for a variety of user types, roles, and groups.
J-01.03	for authorized administrators to assign users to user groups with associated abilities and functionality.
J-01.04	to allow for a variety of user types. E.g. Supplier user, Client user, and System administrator.
J-01.05	to allow for a variety of roles for users. E.g. Admin, Auditor, Finance, Manager, Procurement Officer, Reviewer, Trainer, and "unspecified" user (with full access rights and privileges).
J-01.06	to allow one individual user to be able to have multiple roles, as determined by an authorized administrator.
J-01.07	to restrict users to only access data relevant to their own position in the organizational hierarchy.
J-01.08	for authorized administrators to create, modify and delete user groups; assign users to one or more user groups; and assign, edit, and delete the access rights, functions and privileges of all users at the individual user and the user group level.
J-01.09	for users to identify particular characteristics in their profile with access rights for authorized administrators to review, validate and modify these characteristics.
J-01.10	for authorized administrators to modify the individual settings and characteristics of individual users in groups.

SOW NUM	Requirement
J-01.11	for authorized administrators to delegate their own role to another user for a configurable period of time.
J-02.00	**User Management – Registration** The Contractor must deliver a solution that provides the functionality:
J-02.01	for authorized administrators to create profiles on behalf of users.
J-02.02	to make registration remain incomplete (preventing access to certain solution functionality) until user account configuration is complete.
J-02.03	to transfer information contained within an electronic credential key into the solution for registration purposes.
J-03.00	**User Management - Profiles / Accounts** The Contractor must deliver a solution that provides the functionality:
J-03.01	for authorized administrators to modify, disable, or close individual user profiles in the solution.
J-03.02	to retain user account records within the solution for access by authorized administrators for a defined time period (configurable).
J-03.03	for authorized administrators to clone user profiles for use by new users (authorities, settings, etc.) and modify specific elements of the profiles.
J-03.04	for authorized administrators to manage user accounts once they are created. E.g. Send notifications to users related to account use and functionality.
J-03.05	for authorized administrators to search, display, and modify changes to the profile of any user.
J-03.06	to automatically and regularly send notifications to users to determine the status, and desired status, of their account in the solution.
J-03.07	to automatically close the account of any user who indicates the desired status of their account as such when notified.
J-04.00	**User Management – Login** The Contractor must deliver a solution that provides the functionality:
J-04.01	to require users to authenticate themselves when accessing the system using an electronic credential key.

PART 6: MANAGEMENT AND OVERSIGHT

6.1 CONTEXT

This Section brings together the high-level, cross-cutting requirements from Part 3, the technical requirements from Part 4, and the functional requirements from Part 5 and describes the GC's oversight and contract management expectations.

The Contractor must submit as the basis for reaching the first major Milestone–Delivery of Detailed Final Implementation Plan, as described below. The Contractor must submit the final Implementation Plan for Project Authority approval prior to the go-live date. GC's overall aim is to ensure a consistent approach to training, communications and transition. GC will work jointly with the Contractor to establish an active and ongoing relationship that is essential to achieving the overall EPS objectives.

The Contractor must submit all deliverables described below for Project Authority approval in Microsoft Office formats

6.2 CONTRACT MANAGEMENT PERFORMANCE

The GC has identified specific service level standards and performance measures for the commencement of the Ongoing Operations phase of the Contract described in Part 3, Section 3.7, Service Desk and Section 3.8, Service Management. In subsequent years, standards and measures may be added, modified or removed using the established management structure and framework. The GC will implement metrics for scope, schedule and cost relating to Contract Management and Quality of Service.

6.2.1 Schedule and Progress Metrics

Schedule and Progress Metrics will provide an indication of whether or not the development effort is proceeding as planned. Schedule and Progress Metrics will be used to obtain general information about whether the overall schedule target is being met and to obtain information about specific tasks or parts of the development effort that may be behind schedule.

6.2.2 Cost and Resource Metrics

Cost and Resource Metrics provide an indication of whether the development effort is within cost and whether there are sufficient resources to do the job. Cost and Resource Metrics will be used to obtain information about:

- Whether the overall cost target is being met
- Specific tasks or parts of the development effort that may be over cost
- Resource issues that may cause future problems meeting cost, schedule or technical objectives

6.2.3 Resource Utilization Metric

Resource Utilization Metric is to measure productivity of resources involved in project and be assessed over or under-utilization cases.

Budgeted effort is the planned billable work of resource. Any over-utilization and under-utilization indicated by this metric has an impact on the project's profitability.
This metrics help analyze effort distribution across different project phases/activities. The quality of this metrics improves when a robust time reporting system is available within the organization.

6.3 GOVERNANCE EXPECTATIONS – MANAGEMENT APPROACH

While the formal governance/Contract management structure will only be finalized collaboratively with the selected Contractor following Contract award, it is still important to ensure GC expectations and requirements are clearly understood.

6.3.1 Management/Governance Principles

The Contract management framework and resulting governance mechanism(s) must be defined within the context of the following overarching principles:

- **stewardship**: activities and processes to safeguard money, assets, databases and other knowledge assets and protect them against losses, misuses and waste;
- **transparency:** measureable outcomes-based results, performance metrics and reporting;
- **efficiency/timeliness:** a solution that demonstrates successful, efficient change management and results in improved service delivery; and
- **flexibility:** a solution and delivery of services that demonstrates innovation with a focus on flexibility to accommodate multi-layered change.

6.3.2 Relationship Management Strategy

The Contractor must provide for approval a Relationship Management Strategy that must outline its approach that addresses, at a minimum, the following:

- the overall approach to GC – Contractor relationship management:
- multi-year planning;
- priority setting;
- resource management;
- communications between the delivery partners:
- communicating upcoming changes and their potential impact to the user community (clients and stakeholders);
- multi-channel relationship management;
- issue management and resolution:
- approach to reporting and working with the GC to resolve service standard exceptions, problems and issues, and documentation;
- joint planning and approach to change management:
- proposed terms of reference(s) for any joint committees (including frequency of meetings);
- approach/ methodology to change management, including prioritization, planning and reporting (roadmap);

- a detailed description/approach to justification of eligible additional change management costs (including changes to IP requirements) within the context of the pricing model described in Annex 3: Price Schedule;
- evergreen approach - how hardware, software (applications, database management) and telecommunications) will be kept current and compatible with new technologies, standards, formats and client expectations as part of the Contract commitment to continuous improvement; and
- quality assurance - roles and responsibilities in ensuring quality is maintained in client services and account management processes.

6.3.3 Risk Management

As the provision of other risk management activities identified in the Statement of Work (e.g. audits, insurance) are not intended to cover all of the Contractor's potential requirements in the area of risk management and mitigation, the Contractor must provide for approval additional measures to ensure that it can manage all the risks associated with the delivery of the Contract.

More specifically, the Contractor must establish a proactive, systematic and continuous process to identify, access and manage risks associated with the performance of the Contract. As such, the Risk Management Strategy must outline the risk management approach that addresses, at a minimum, the following items:

- the development of an ongoing, annual risk management plan;
- the completion of an annual Threat and Risk Assessment;
- an initial baseline assessment of key risks;
- the identification of mitigation strategies for key risks including an action plan for mitigating;
- a proposed tool or system to track risks during all phases of the Contract and attendant mitigating strategies; and
- a continuous risk management strategy.

6.3.4 Three Year Technology Road Map

The Contractor must provide for approval a Technology Road Map during transition and throughout the Contract period to describe how the EPS will be maintained and upgraded over the duration of this Contract. The Contractor must provide their 3-year technology road map, updated annually, including key product road map for their proposed EPS that incorporates, at a minimum the following:

- how the Technology Road Map will address the business objective and needs of the EPS over the life of the Contract;
- strategy to accommodate the evolution of technological advancement to update and maintain its technology current;
- address software**:** Compatibility, Availability, Interoperability, licensing (if applicable), and administration;

- differentiates between standard regular upgrade cycles to keep the proposed solution design current and actual proposed solution design change;
- how the Contractor will use the Technology Road Map to make resource allocation decisions;
- previous successful use and reference of the main products in the proposed solution design for project of a similar nature; and
- description of investments made by the Contractor in order to keep the solution current

6.3.5 Project Management Reporting

6.3.5.1 General

The Contractor must produce and submit to the Project Authority quarterly for review, management reports on performance of the project. Management reports must be sufficiently comprehensive to provide "Planned Value" and "Demonstrated Value" comparison reports and must contain data derived from the Contractor's Contract Work Breakdown Structure and Contract management control system with a clear, verifiable trail of derivation. GC requires summary reports only, but the Contractor must provide details upon request, or if problems require corrective action.

6.3.5.2 Kick-off Meeting

The Contractor must organize a kick-off meeting with the Project Authority in the National Capital Region (NCR), within 10 (ten) business days from the date of Contract Award.

The purpose of the kick-off meeting as a minimum will be to:

i. Review the contractual requirements;
ii. Review and clarify, if required, the respective roles and responsibilities of the Contracting Authority, the Project Authority and of the Contractor to ensure common understanding; and
iii. Discuss the Project Plan.

The Contractor must prepare and submit the minutes of the meeting within fifteen (15) business days to the Project Authority for concurrence/approval. The minutes of the meeting will provide the names of all attendees, a record of discussions and decisions made. Any required changes will be discussed between the Project Authority and the Contractor.

6.3.5.3 Weekly Status Meetings

The Contractor must organize, schedule and conduct weekly status meetings with the Project Authority in the NCR throughout the Contract period, at the discretion of the Project Authority. The focus of these meetings must be to update the Project Authority on key aspects of the EPS project.

The Contractor must prepare and submit the minutes of the meeting within five (5) calendar days to the Project Authority for concurrence/approval. The minutes of the meeting will provide the names of all attendees, a record of discussions and decisions made. Any required changes will be discussed between the Project Authority and the Contractor.

6.3.5.4 Monthly Project Progress Report

The Contractor must prepare and present a monthly Project Progress Status Report to the Project Authority. This report must contain the following information:

- overall project status;
- a summary of key project activity and the associated expenses;
- statistical volumetric information;
- named user license count report
- a summary of service level performance;
- a list and a description of major events;
- risk status; and
- client satisfaction survey results.

6.3.5.5 Strategic Management Semi-Annual Reviews

The Contractor must prepare and present to the Project Authority, a Semi-annual Review including presentations of all service components. The semi-annual review must include the following:

- Project status, including status of key problems.
- Issues that the service is currently facing and a proposal on how to address them.
- Risk management status.

6.3.5.6 Delivery of Project Documents

Within 30 business days of Contract award, the Contractor must provide for Project Authority approval a schedule of documents that will be delivered during all phases of the Contract at a minimum; this schedule must contain the following information:

- document name;
- description
- version number;
- frequency of document creation and delivery;
- draft delivery date;
- amount of time (in days and/or minutes) for the Government of Canada (GC) to review and approve the document; and
- final delivery date

6.4 OPERATIONAL READINESS

6.4.1 Project Management Office

The Contractor must staff and operationalize a project management office for the Contract Period at a Contractor's location within 10 business days of Contract award to:

- Ensure overall coordination of all project related activities under the EPS Contract

- manage the resolution of EPS project issues, problems and complaints, and escalate and prioritize project issues as requested by GC;
- provide a project manager who will function as GC's single day to day point of contact for the project management office; and
- provide a telephone number in the National Capital Region (NCR) and email address to contact the project management office 8:00 to 17:00 ET, during working days

6.4.2 Operational Readiness Plan

The Contractor must submit a draft operational readiness plan within 45 business days after Contract award for approval by GC that identifies a schedule in Microsoft Project format to complete the project plans and work required in this SOW. For each project plan the Contractor must:

- include a Responsible, Accountable, Consulted, and Informed (RACI) chart to identify the roles and responsibilities for key Contractor, GC and any Third Party Member involved for the successful execution of the plan;
- provide a list of task dependencies;
- not create unnecessary dependencies on GC's review and approval;
- identify the phases, gates, deliverables and milestones of the Work as distinct tasks where each task has a start and end date, a duration, is assigned to a resource group, and has the dependencies identified, such that the start and end date of the tasks are driven by the dependencies, duration and resources;
- identify each Contract deliverable as a milestone;
- schedule tasks in parallel to the maximum extent possible;
- provide a list of planning assumptions;
- Identify schedule risks including:
    - categorization of each risk;
    - probability of each risk;
    - impact if the risk materializes;
    - mitigation measures;
    - monitoring measures; and
    - risk assignment
- provide a complete list of the functionality for each software proposed

The Operational Readiness Plan will cover the work required to complete the following plans:

1. Project Management Plan;
2. Overall Transition Plan;
3. Change Management and Communications Plan;
4. Supplier Enablement Plan
5. Functional Requirements Traceability Matrix;
6. Service Management Guide including:
    - management and operational structure, organizations, roles and responsibilities of each function performing work under this Contract and key personnel and subject matter experts;

- operational and management escalation process that includes:
    I. identification of the designated GC and Supplier personnel authorized to invoke the escalation procedure;
    II. escalation contact names, titles, EPS addresses and phone numbers; and
    III. escalation time frames based on the length of time an Incident remains unresolved and priority of the Incident;

7. Privacy Management Plan;
8. Privacy Impact Assessment;
9. Feature list that includes a mapping of the bidders solution to parts 3,4, and 5 based on user manuals and/or systems specification document;
10. Configuration Management Plan;
11. Service Design and management;
12. Service Continuity Plan;
13. Implementation Plan of the EPS Services;
14. Network Design;
15. Security Design.

The Work identified in the operational readiness plan must be completed according to:

- PWGSC will review the draft operational readiness plan within ten (10) business days;
- The Contractor must provide an updated operational readiness plan according to feedback received from PWGSC within five (5) business days after receiving the feedback; and
- PWGSC will review the final operational readiness plan within five (5) business days. .

Unless otherwise specified, for each deliverable in the draft operational readiness plan:

- PWGSC will review the draft deliverable within 10 business days;
- the Contractor must provide updated deliverables according to feedback received from PWGSC within five (5) business days after receiving the feedback;
- PWGSC will review the deliverable within five (5) business days ; and
- the Contractor must provide final deliverables according to feedback received from PWGSC within five (5) business days after receiving the feedback.

6.4.3 IT Security Plan

The IT Security Plan should include an Implementation plan which describes how the requirements will be addressed in alignment with the PWGSC Security Assessment and Authorization (SA&A) process. The PWGSC Security Assessment and Authorization process is comprised of three gates plus the operational state which provide assessment opportunities at different levels of granularity. It is important to note that all security requirements must be traced from High-level design (Gate 1) to Integrate & Test (Gate 3) and finally operations. As well, since the controls are dependent upon the solution architecture, it is important to note that it is expected that the controls at each Gate will be refined during the SA&A process.

6.4.4 PWGSC Security Assessment and Authorization (SA&A) Process

6.4.4.1 Security Assessment and Authorization Gate 1

The Contractor must complete the following Work for SA&A Gate 1, within ## business days of Contract award (to be specified by the Contractor in the IT Security Plan submission), which includes GC approval:

a. Security High Level Service Design (SHLSD); and
b. Security Requirements Traceability Matrix (SRTM).

The Contractor must provide a SHLSD to GC that includes:

a. a high-level component diagram that clearly shows the allocation of services and components to network security zones and identifies key security related data flows;
b. the architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer);
c. a description of the network zone perimeter defences;
d. a description of the use of virtualization technologies, where applicable;
e. descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;
f. descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements;
g. a description of the approach for:
    i. remote management;
    ii. access control;
    iii. security management and audit;
    iv. configuration management; and
    v. patch management.

The Contractor must provide a SRTM to GC that includes for each requirement in Annex 2 Security Requirements:

a. the security requirement identifier (E2.## as identified in the Annex 2 for each of the security requirement);
b. an identifier that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line identifier);
c. the security requirement statement;
d. a description of how the security requirement is addressed in the Security High-Level Design in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements;
e. the title of the Contract deliverable(s) in which the Contractor will provide the details of its security solution for the requirement (e.g., service continuity plan); and
f. tracing (a reference to an identifiable element) to the Security High-Level Service Design to allow Canada to confirm that the security safeguards satisfy the security requirements

6.4.4.2 Security Assessment and Authorization Gate 2

The Contractor must complete the following Work for SA&A Gate 2, within ## business days (to be specified by the Contractor in the IT Security Plan submission) following acceptance of the Work for SA&A Gate 1, which includes GC approval for:

a. Security Detailed Service Design (SDSD);

b. Security Requirements Traceability Matrix (SRTM);
c. Change Management Procedures;
d. Operational Security Procedures; and
e. Security Installation Procedures.

The Contractor must provide a SDSD to GC that includes:

a. a detailed component diagram (this must be a refinement of the high-level component diagram);
b. descriptions of the allocation of technical security mechanisms to detailed service design elements;
c. descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements; and
d. justification for key design decisions

The SDSD must comply with the Security High-Level Service Design.

The Contractor must update the SRTM to include the following information for each security requirement in Annex 2 Security Requirements:

a. the security requirement identifier (E2.## as identified in the Annex 2 for each of the security requirement);
b. an identifier that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line identifier);
c. the security requirement statement;
d. a description of how the security requirement is addressed in the Security Detailed Level Design in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements;
e. the title of the Contract deliverable(s) in which the Contractor will provide the details of its security solution for the requirement (e.g., service continuity plan); and
f. tracing (a reference to an identifiable element) to the Security Detailed Level Service Design to allow Canada to confirm that the security safeguards satisfy the security requirements

The Contractor must provide Change Management Procedures to GC that includes:

a. Contractor's change management authorities;
b. Contractor resource roles and responsibilities for change management;
c. how the Contractor will use the change management process to support the development of the EPS;
d. method used to uniquely identify configuration items;
e. configuration item identification method;
f. description of the change management process, including the change review and approval process;
g. means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items;
h. measures used to enforce only authorized changes ; and
i. procedures that the Contractor will use to accept modified or newly created configuration items.

The Contractor must provide Operational Security Procedures to GC that includes:

a. for each operator role:
    i. schedule of security-relevant actions to be performed in order to maintain the security posture of the EPS;

ii. how to use available operational interfaces; and
iii. each scheduled action and how the user is expected to perform it.

b. operational roles and responsibilities for:
i. interaction requirements with PWGSC representatives;
ii. reporting schedule and procedures;
iii. access control;
iv. audit and accountability;
v. identification and authentication;
vi. system and communications protection;
vii. awareness and training;
viii. configuration management;
ix. contingency planning;
x. incident response;
xi. maintenance;
xii. media protection;
xiii. physical and environment protection;
xiv. personnel security; and
xv. system and information integrity.

The Contractor must provide Security Installation Procedures to GC that includes:

a. steps necessary for the secure installation and configuration of Service Portal;
b. installation and configuration of all technical security solutions;
c. security configuration of Hardware products; and
d. security configuration of software products (COTS and open source).

6.4.4.3 Security Assessment and Authorization Gate 3

The Contractor must complete the following Work for SA&A Gate 3, within ## business days (to be specified by the Contractor in the IT Security Plan submission) following acceptance of the Work for SA&A Gate 2, which includes GC approval for:

a. Security Installation Verification Plan;
b. Security Installation Verification Report;
c. Updated SRTM with Security Installation Verification mapping to security requirements;
d. Security Integration Test Plan;
e. Security Integration Test Report;
f. Updated SRTM with Security Integration Test Report mapping to security requirements;
g. Vulnerability Assessment Plan;
h. Vulnerability Assessment Report; and
i. Updated SRTM with Vulnerability Assessment Report mapping to security requirements;

6.4.4.4 Security Installation Verification

The Contractor must provide a Security Installation Verification Plan to GC that must include:

a. the security verification approach;
b. Canada witnessing arrangements;
c. an outline of the security verification items; and
d. for each security verification item:
i. a description of the verification scenario;
ii. ordering dependencies; and
iii. expected results (i.e., pass/fail criteria).

The Contractor must provide an updated SRTM to GC that includes for each security requirement to be tested by the Security Installation Verification Plan, the tracing (a reference to an identifiable element) to security installation verification test cases.

The Contractor must conduct security installation verification in accordance with the approved Security Installation Verification Plan.

The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

The Security Installation Verification Report must include for each of the test items in the security installation verification plan:

a. the expected results (i.e., pass/fail criteria);
b. the actual results; and
c. a description of deviations and how each was resolved.

6.4.4.5 Security Integration

The Contractor must provide a Security Integration Test Plan to GC that must include:

a. the security functions to be tested;
b. GC witnessing the testing arrangements; and
c. for each security function or sets of security functions, the items to be tested, including:
    i. a description of the test case, procedure, or scenario;
    ii. environmental requirements;
    iii. ordering dependencies; and
    iv. expected results (i.e., pass/fail criteria).

The Contractor must provide an updated SRTM to GC that includes for each security requirement to be tested by the Security Integration Test Plan, the tracing (a reference to an identifiable element) to integration security testing test cases.

The Contractor must conduct security integration testing in accordance with the Security Integration Test Plan.

The Security Integration Test Report must include, for each of the test items in the Integration Security Test Plan:

a. the expected results (i.e., pass/fail criteria);
b. the actual results; and
c. a description of deviations and how each was resolved.

6.4.4.6 Vulnerability Assessment

The Contractor must provide a Vulnerability Assessment Plan that must include:

a. a description of the scope of the vulnerability assessment;
b. GC witnessing arrangements;
c. a description of the vulnerability assessment process; and
d. a description of the vulnerability assessment tools that will be used, including any software versions.

The Contractor must conduct a vulnerability assessment in accordance with the approved Vulnerability Assessment Plan.

The Contractor must implement patches and corrective measures as part of vulnerability assessment activity. Where this is not feasible (e.g., time to test patch or determine and test corrective measures would seriously delay the project), the Contractor must create Service Request Tickets for any required patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity.

The Vulnerability Assessment Report must include:

a. a listing of the vulnerability assessment tests that were conducted;
b. all raw data for the results of the vulnerability assessment tests in a COTS file formats and names specified by Canada;
c. for each vulnerability assessment test:
    i. whether a known vulnerability was detected;
    ii. a description of the vulnerability; and
    iii. a description of the patch or corrective measure that was implemented to resolve the vulnerability.
d. for any unresolved vulnerability:
    i. an assessment of the significance of the vulnerability in the context of the Workplace Communication Services; and
    ii. the problem ticket number for the outstanding patch or corrective measure; or
    iii. the rationale for not implementing a patch or a corrective measure.

6.4.5 Project Management Plan

The Contractor must provide a project management plan which must address the following topics:

- Executive summary description of GC EPS Services;
- Organizational plan that includes management structure, organizations, and roles and responsibilities of key personnel and subject matter experts;
- Resource plan that includes a methodology for determining resource levels required to complete the Work under the Contract and for assessing the skills and competencies of the resources to perform the required function;
- Contract Work Breakdown Structure which must show the relationships between hardware, software, and all related services in the planning and control of cost, schedule and technical performance. The relationship between the Contract Work Breakdown Structure and organizational responsibilities must be explained.
- Contract management Control System which must support the planning and controlling of cost, schedule, and technical performance, and to report accurate status against plan, and to forecast results of alternative project actions. The system must be extended to cover subcontractors' work; Subcontract Management Plan that identifies the working relationships between the different entities involved in the work. Project Schedule management which will clearly identify activities, events, and their logical or technical links required for the achievement of key project milestones, and will clearly relate to the Contract Work Breakdown Structure and the contract management control system;

- System Engineering Management Plan, which must ensure that the elements of the CWBS and technical tasks are correctly identified and controlled, and that the design is complete in its response to all stated needs of GC. It must describe how the requirements are mapped to the planned design and service offering; outlines supporting evidence for claimed performance and scalability; and outline how the responsibility of technical requirements will be distributed among the supplier, its subcontractors, and GC; and a description of the formal design and configuration review process including roles and responsibilities of subcontractors;
- Quality assurance plan that includes an approach to formulating and enforcing work and quality standards, and reviewing work in progress;
- Risk management plan that includes the approach for identifying and tracking risks, isolating the event triggers for risks, assessing probability and impact, as well as identifying a mitigation plan; and
- Issue management plan that includes the approach for identifying and managing service management issues, isolating the issues, assessing the impacts, identifying responsible parties, assessment of a severity and priorities, and processes for determining a resolution.

6.4.6 Overall Transition Plan

The overall transition plan must identify separate and distinct waves as defined below of EPS deployment that will aim to facilitate the retiring of the legacy systems, facilitate transformation of the procurement operations and efficiently and effectively manage the change in GC.

The Contractor must submit an overall transition plan for coordinating all activities related to EPS rollout within 30 business days of Contract Award, for approval by GC that identifies a schedule in Microsoft Project format to complete the following work:

6.4.6.1 Wave 1 Transition

The following requirements must be completed within 8 months of Contract award

- General Requirements as described in table 94 in Part 5 Functional Requirements
- Portal capabilities as described in Part 5 Functional Requirements,
- Supplier Enablement
- Supplier Relationship Management as described in Part 5 Functional Requirements
- GC User Registration with User Management as described in Part 5 Functional Requirements
- support model during transition to integrate and operationalize Service Desks and address problems with GC user and supplier registration; and an issue escalation process.

6.4.6.2 Wave 2 Transition

The following requirements must be completed within 18 months of Contract award
PHASE 1 – limited rollout to a controlled area within PWGSC with specific functionality
The following functionalities will be rolled out:

- Sourcing and Contract Management as described in Part 5 Functional Requirements
- Workflow and Workload Management as described in Part 5 Functional Requirements
- Procurement Management as described in Part 5 Functional Requirements

- Business Intelligence as described in Part 5 Functional Requirements
- Vendor Performance as described in Part 5 Functional Requirements
- support model during transition to integrate and operationalize Service Desks and address problems with Users; and an issue escalation process.

PHASE 2 – The functionalities listed in Phase 1 - Rollout to the PWGSC Department

6.4.6.3 Wave 3 Transition

The following requirements must be completed within 24 months of contact award
PHASE 1 – Limited rollout to selected GC Departments.
The following functionalities will be rolled out:

- Procurement Management as described in Part 5 Functional Requirements
- Sourcing and Contract Management as described in Part 5 Functional Requirements if required
- Vendor Performance as described in Part 5 of the Functional Requirements:
- Service Procurement as described in Part 5 Functional Requirements
- Government Electronic Tendering System (GETS) as described in Part 5 Functional Requirements
- Application Integration Support; and
- Transition reporting

PHASE 2 – The functionalities listed in Phase 1 – Rollout to all GC Departments

The work identified in the overall transition plan must:

- identify when the Transition Plan will be completed
- develop a checklist of pre-transition activities (such as the prioritization of user on boarding, identity attributes to be migrated, data preparation, application integration deployment strategy, network readiness, etc.);
- develop a checklist of post-transition activities;
- develop a detailed schedule;

6.4.7 Change Management and Communications

The Contractor must provide a change management plan within 60 Business Days of Contract award, for approval by the Project Authority that includes the following material:

1. Communication Plan that includes:
   High level awareness communications kit which includes:
   - communicating program benefits of the GC EPS Service;
   - communicating how the GC readiness activities will be accomplished;
   - communicating how Users can support the GC transition effort, and
   - post-migration assessment to aid in future transition activities.

2. Training Plan that includes:
   - material, logistics and schedule that could include:

- Training Approach;
- Training Requirements Assessment by User Class. This must address the initial training requirement for the e-Procurement Solution to "go live" and the ongoing training requirement for new users or refresher training;
- Training Requirements for Administration Access.
- Please refer to table 115 for further requirements on Training Plan

The training plan for Users must include:

- scheduled communications based on the User's migration date;
- instructions on locating training resources;
- details on expected User outcomes;
- detailed instructions on each transition approaches including:
- tools and resources that will be available;
- how to populate user profiles;
- frequently asked questions; and
- instructions on providing feedback during the transition.

The training plan for level 1 service desk must include:

- schedule of transition activities;
- description of access rights and roles and responsibilities of level 1 service desk agents during the GC migration;
- instructions on locating of support material;
- escalation procedures.

The training plan for GC Administrators must include:

- schedule of transition activities;
- description of access rights and roles and responsibilities of GC and GC Administrators during the GC migration;
- instructions on locating of support material.

3. schedule of activities before, during and after transition activities;
4. expected outcomes;
5. identifying when, for how long, and the type of GC resources that are required for change management; and
6. change management reporting.

The Contractor must provide change management reporting that collects and reports against each PWGSC's overall transition status including statistics for:

a. Identity Profiles created and number of users successfully on-boarded (total, percentage);
b. Calls to the Service Desk related to transition activities; and
c. Percentage of completed post migration feedback forms.

The Contractor must ensure the change management plan integrates with the operational readiness phase plan and wave schedules.

The Contractor must commence the execution of the activities as identified in the change management plan, according to the defined schedule, at least 30 Business Days before the first scheduled transition activity.

6.4.8 Supplier Enablement Plan

In this section a number of mechanisms, strategies and events are detailed and mapped to the expectations articulated in Part 6. During project implementation further items may be added.

The Contractor must provide a supplier enablement plan that outlines:

- **Awareness:** design a strategy so suppliers develop knowledge of the change. The strategy should address the main objectives of the change, and when and how it should be met.
- **Understanding:** ensure suppliers comprehend the nature and intent of the change and start to develop an understanding of what this will mean for them. The Contactor will be responsible for communication to the Supplier community on changes to how they do business with GC and what needs to be met to reach implementation.
- **Positive Perception:** build and implement strategies and interaction models to engage suppliers in developing a readiness to change.
- **Implementation:** support processes, guidance and systems to ensure that the change is fully operationalized across the supplier community. A proposed schedule to meet a fully operationalized change will be included.
- **Adoption:** The change has been operational for long enough to evaluate its worth and impact. The evaluation of the project will be ongoing. However, once the change is fully operationalized, an evaluation will provide worth and impact.

While particular communication events and strategies will be developed to support suppliers through these phases and in relation to their expectations, the Contractor must support a range of regular and ongoing initiatives that will be employed to monitor supplier expectations, feedback and attitudes.

6.5 TRANSITION SERVICES

6.5.1 Context

While the management principles identified in 6.2 are applicable throughout the duration of the Contract, including the three distinct phases (Set-up/Transition in, Ongoing Operations and Close-out/Transition-out) identified below, it is understood that the majority of the functional requirements for administering EPS will occur during the Ongoing Operations phase.

The Contract has three distinct phases:

6.5.2 Setup/Transition-in Phase

This phase includes all activities required to implement the EPS. This include all activities required to develop a transition project plan, activities associated with the preparation of the EPS environment, data conversion and migration, integration and testing activities, and organization change management & training and support. This phase also includes:

- discovery research and assessment to determine specific requirements for processing various components of the service;
- testing operational solutions;
- onboarding legacy data
- developing solution specific guidelines; and
- developing operational procedure documentation, as required

6.5.3 Transition-In

6.5.3.1 Approach

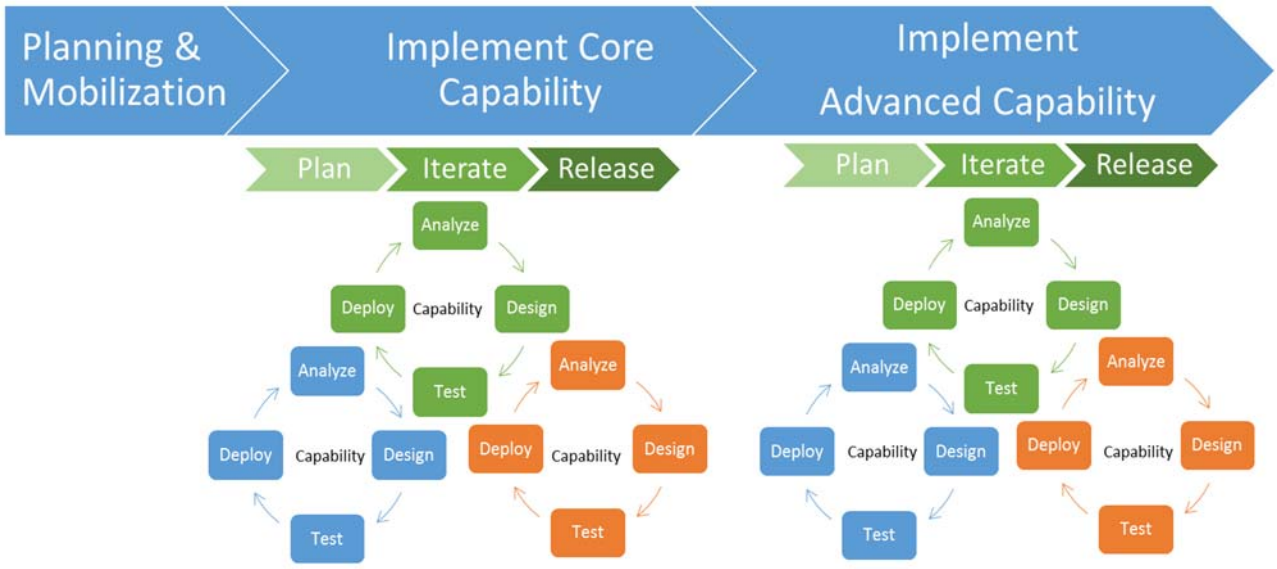
GC will take a proactive, milestones-based approach to managing transition-in and given the size and complexity of the activities required to ensure a smooth transition-in, it will be essential for PWGSC and the Contractor to take a collaborative and agile approach to implementation.

The Contractor must conduct a high level assessment of PWGSC's current state and identify areas of change, including key business processes. The Contractor must use existing business objectives, best practice, and customer input to establish goals, a vision, and a set of principles in each domain of change. These goals must drive planning, standardization and alignment for specific areas of the business, resulting in an organization positioned for change.

The transition-in phase defines the overall business solution, in terms of integrated high-level components, in sufficient detail for development work to begin. In addition, business architecture is developed with the eventual operational service in mind, to ensure that the operational performance goals and expectations are met.

Implementation planning must focus on delivering a rapid return on investment by creating a "continuous flow of value", that is, capability is expected to be delivered in an iterative fashion to allow the GC to begin benefiting from EPS immediately. The Implementation Plan must be based on an approach that divides the overall solution into manageable releases that can be implemented rapidly.

Figure 7 - Sample Agile Approach



6.5.3.2 Implementation Plan – Setup/Transition-in

Within the context of the Transition-in and as part of the Implementation Plan, the Contractor must describe and identify their overall management approach, including but not limited to:

- identification of appropriate resources to complete all major milestones;
- the proposed Project Management Approach to reach each milestone;
- a proposed Risk management and Issues Resolution Approach; and
- high-level implementation schedule complete with a brief description of the key activities, risks and mitigation strategies within each of the major transition milestones.

6.5.3.3 Setup/Transition-in - Users

In accordance with the objectives in Part 1 of the Statement of Work, the Contractor's implementation plan must focus on the strategic approach to offering the EPS to users, and transitioning users from existing processes to electronic processes. At a minimum, the detailed Final Implementation Plan must also identify and describe:

- outline the services and proposed solution deliverables within the context of the functional and high level requirements; and
- how the Contractor will onboard each of the user communities..

6.5.3.4 Transition Planning

Activities required to develop a Transition Project plan with input and agreement from all stakeholders.

Table 109 - Transition Planning Roles and Responsibilities

Transition Planning Roles and Responsibilities	Contractor	GC
Prepare project plan to support integrated Transition planning and execution.	R	A
Approve project plan.	I	R
Provide appropriate skill level and trained Contractor personnel for Transition.	R	A
Identify high risk Transition areas and impact, develop mitigation strategies, and recommended mitigation actions and report results to GC.	R	A
Review risk mitigation plan(s) and determine with Contractor's assistance which mitigation strategies and courses of action to approve, if any.	C	R
Document baseline including high-level process maps, standard operating procedures and baseline user service levels and operational activities for use in Transition planning, readiness, cutover and stabilization activities.	R	A
Develop, update, maintain, and revise, a detailed Transition plan(s) that includes approach, activities, milestones, schedule and risk identification and mitigation strategies.	R	A
Approve Transition Project plans, schedules, and related documentation, including all plan revisions.	I	R
Provide status reports and risk mitigation plans weekly.	R	A

6.5.3.5 Infrastructure Transition

This includes all activities necessary to transition support of all in-scope systems.

Table 110 - Infrastructure Transition Roles and Responsibilities

Infrastructure Transition Roles and Responsibilities	Contractor	GC
Perform Knowledge Transition with GC, Contractors and/or Current Service Contractors.	R	A
Document system administration and database administration tasks in a knowledge management database to optimize information collection and organization.	R	A
Work with current Contractor(s) and GC to support the transition plan milestones.	C	R

6.5.3.6 Transition and Migration

This includes all activities associated with the preparation of the GC environment for Transition.

Table 111 - Transition and Migration Roles and Responsibilities

Transition and Migration Roles and Responsibilities	Contractor	GC
Execute Transition Plan(s).	R	A
Provide the Program Office Transition status report(s).	R	A
Manage, update, and maintain detailed Transition schedule(s) that includes activities, deliverables, milestones, and dependencies/linkages to Current Service Contractor schedules.	R	A
Develop, identify and report on Transition schedule critical path activities on a weekly basis and escalate issues as required to GC.	R	A
Provide standardized processes and templates using automated tools whenever possible, which at minimum includes: • Risk log; • Issue log ; • Integrated Milestone Schedule; • Status report/performance report; • Change control processes/templates; • Communication processes; • Change Management (Training, etc.); and • IT Knowledge management/document repository tools.	R	A
Approve processes and templates.	I	R
Develop a thorough implementation readiness assessment plan, readiness assessment schedule, rollback strategy, assessment scorecards, identified and defined critical readiness criteria that will drive go/no-go decisions related to overall readiness/preparedness for going live with any new service or IT environment.	R	A
Approve readiness assessment plan.	I	R
Conduct implementation readiness assessments and report findings and recommendations on a weekly interval basis prior to cutover and identify any items or situations that will impede successful cutover.	R	A
Perform and complete remediation actions based on readiness assessments and report status to GC.	R	A
Verify that all work, testing, evaluation, assessments, and corrective remediation activities are performed and successfully completed to ensure GC achieves 100% implementation readiness for all implementation criteria prior to going live.	R	A
Develop necessary stakeholder communications in accordance with GC Communications Policy during pre-implementation.	R	A
Review and deploy stakeholder communications during pre-implementation.	C	R
Collect, analyze and report stakeholder feedback issues, comments and/or requests.	C	R
Provide recommendations on best course(s) of actions to take to address/resolve stakeholder issues.	R	A
Review stakeholder report and authorize acceptable resolution actions.	C	R

Develop a detailed implementation plan, including a pre-implementation checklist and post-implementation measurable evaluation criteria for the e-Procurement Solution.	R	A
Review and approve the implementation plan.	I	R
The Contractor must implement their service in a phased approach in departments as specified by GC on the go-live date.	R	A
The Contractor must complete all implementation activities within the timeframes stipulated in the finalized Implementation Plan.	R	A
Develop a detailed implementation plan, including a pre-implementation checklist and post-implementation measurable evaluation criteria that will assist participating departments, agencies and crown corporations in preparing for the implementation and deployment of the service.	R	A
Make go/no-go recommendations and prepare an implementation decision document for approval.	R	A
Develop necessary stakeholder communications in accordance with Government of Canada Communications Policy during implementation.	R	A
Review and deploy stakeholder communications during cutover.	I	R
Collect, analyze and report stakeholder feedback issues, comments and or requests.	C	R
Review stakeholder report and authorize acceptable resolution actions.	C	R
Manage implementation and cutover in accordance to plan with no disruption to GC service delivery.	R	A
Complete all post-cutover activities per cutover plan ensuring 100% completion of post-cutover activities.	R	A

6.5.3.7 Transition Integration and Testing

This is to ensure the right testing plans and requirements are in place to support the testing services necessary to ensure an effective transition.

Table 112 - Transition Integration and Testing Roles and Responsibilities

Transition Integration and Testing Roles and Responsibilities	Contractor	GC
Provide proposed integration, test strategy and plan to verify functional, performance, and reliability requirements.	R	A
Review and approve integration and test strategy and plan.	I	R
Recommend integration and testing requirements.	R	A
Approve integration and testing requirements.	I	R
Develop, document and maintain integration and testing plan that meets requirements and adheres to defined policies.	R	A
Manage integration test environment. The Contractor must provide a testing environment exclusive to PWGSC accessible through the Internet. The testing environment will be used by PWGSC for testing on a continuous, non-scheduled basis to support on-going testing of their applications.	R	A

• Functionality: maintained with production-like code at all times, and updated with current configurations during testing sessions scheduled with the Contractor. • Availability: twenty-four (24) hours per day, seven (7) days per week, except for any regularly scheduled maintenance window not exceeding 4 hours a week and reductions imposed on the Contractor to debug problems. • Support: from 7:00 to 20:00 ET, Monday to Friday, excluding statutory holidays. • Incident and Problem Management: priority-based response to testing environment incidents during normal business hours. If an incident is not resolved by 20:00 ET on a given day or occurs outside of normal support hours, problem resolution is to continue at 7:00 ET on the next business day.		
The Contractor must provide support for testing activities to the GC when there are modifications or updates to the e-Procurement Solution.	R	A
Maintain Software release matrices across development, quality assurance, and production environments and Networks.	R	A
Conduct integration and security testing for all Data, Equipment, or Networks based on requirements defined in the plan and GC policies and procedures.	R	A
Evaluate all new and upgraded System components and Services for compliance with GC security rules, regulations and procedures.	R	A
Provide proposed integration and test plan.	R	A
Assess and communicate the overall impact and potential risk to system components prior to implementing Changes.	R	A
Define User Acceptance Testing (UAT) requirements.	C	R
Develop User Acceptance Testing plans per requirements.	C	R
Review and approve User Acceptance Testing plans.	C	R
Conduct and document User Acceptance Testing results per requirements.	R	A
Review and approve User Acceptance Testing results.	C	R
Stage new and upgraded Equipment, Software or Services to smoothly transition into existing environment based on requirements defined in requirements.	R	A
Conduct User Acceptance tests.	I	R
Share User Acceptance test results with Contractor.	C	R
Assess and communicate the overall impact and potential risk to system components prior to implementing Changes.	R	A

6.5.3.8 Program Stabilization and Post-transition

These are the services necessary to support the organization following the transition in order to help it achieve a steady state.

Table 113 - Program Stabilization and Post-Transition Roles and Responsibilities

Program Stabilization and Post-Transition Roles and Responsibilities	Contractor	GC
Resolve any stabilization/post-cutover issues identified by GC as highest-priority within five (5) days of cutover.	R	A
Conduct post-cutover inspection and submit completed post-cutover checklist within five (5) days following cutover.	R	A
Conduct a stabilization assessment within ten (10) days following cutover including analysis and recommendations.	R	A
Complete all stabilization activities within 30 days following cutover.	R	A
Develop necessary stakeholder communications immediately following cutover.	R	A
Deploy stakeholder communications immediately following cutover.	I	R
Collect, analyze and report stakeholder feedback issues, comments and or requests.	R	A
Conduct a post-Transition review within 60 days of cutover.	R	A
Provide a Transition-In Lessons Learned Report for Project Authority approval no later than 90 days after the go-live date based on all lessons learned from the execution of the Transition-In Implementation Plan.	R	A
Incorporate lessons learned into subsequent Transition activities (e.g., future transitions, transition-out planning, etc.).	R	A
Develop necessary stakeholder communications during post-Transition.	R	A
Review and deploy stakeholder communications during post-Transition.	I	R
Collect, analyze and report stakeholder feedback issues, comments and or requests.	R	A

6.6 ONGOING SUPPORT PHASE

This phase refers to the point in which the service is underway (go-live) delivering the EPS, monitoring and performing changes and enhancements where required, providing on-going organizational change management, training and support, and responding to adjustments.

6.6.1 Ongoing Support

This is the day-to-day operational activities required to support effective management of the EPS and the production environment in which it operates. These activities include, but are not limited to, problem management, incident management, change management, communication and escalation procedures, and regular management reporting.

Table 114 - Program Stabilization and Post-Transition Roles and Responsibilities

Ongoing Support Roles and Responsibilities	Contractor	GC
Provide documented tools and processes to provide the necessary support for its EPS, particularly in the following areas: • incident and problem management; • change management; and • communication and escalation procedures.	R	A
Schedule a regular maintenance period per week and the maintenance period must be non-intrusive to the production environment unless advance notice of four (4) weeks is provided.	R	A
Provide status reports detailing progress and updates to the ongoing support.	R	A

6.6.1.1 Organizational Change Management & Training Support

This is for the GC's EPS Transition, which includes thorough technical and End User training, effective communication and successful stakeholder participation.

Table 115 - Organizational Change Management & Training Support Roles and Responsibilities

Organizational Change Management & Training Support Roles and Responsibilities	Contractor	GC
Conduct Training and Change Management Strategy & Objectives.	C	R
Develop a training plan, material, logistics and schedule that could include: • Training Approach; • Training Requirements Assessment by User Class. This must address the initial training requirement for the e-Procurement Solution to "go live" and the ongoing training requirement for new users or refresher training; • Training Requirements for Administration Access.	R	A
Revise/Update Training material annually or concurrent with a major release to address new features and release changes. Training Materials must comply with the approved Training Plan.	R	A
Approve the Training Plan and material.	I	R
Provide training module content that is copyright and royalty free for modification and redistribution by Canada.	R	A
Conduct Change Management Training/Knowledge Transfer.	R	A
Executing Training and Organizational Change Management plan.	C	R
Conduct Audience/Trainee Analysis.	C	R
Conduct Technical Administrator Training.	R	A
Conduct End User training for suppliers.	R	A
Conduct Train the Trainer Training for procurement specialists as defined by GC.	R	A
Provide role-specific training to Project Authority staff prior to each new product version release.	R	A
Inform and educate client departments and end users about the end-to-end solution that will support their business requirements.	R	A

Organizational Change Management & Training Support Roles and Responsibilities	Contractor	GC
Keep our clients abreast of the latest trends, developments and new occurrences.	R	A
Disseminate information on upgrades, enhancements and improved functionality to our target audience.	R	A
Manage Communication Vehicles.	C	R
Manage Communication Schedule/Frequency.	C	R
Develop Change Management Metrics.	C	R
Organizational Transition (e.g., training, new process flows, reclassification).	C	R

6.7 CLOSE-OUT/TRANSITION-OUT PHASE

This phase refers to the point at which the Contractor prepares to transition required deliverables; resources, documentation and client information in support of the initiation of the next Contract. The Contractor must continue ongoing support during the close out/transition-out phase.

6.7.1 Contract Phases – Close-out/Transition-out

Transition Out to facilitate with the transition to a new service (to a new Contractor or to an internal GC entity). This includes, but is not limited to, the migration of all EPS data to the GC's new service. The Contractor must provide the GC with the information necessary to map the existing EPS's data to the GC's new service. The roles and responsibilities are listed in the following table. Two transition options are further elaborated in the following section –Future In-Scope Service Transition Support (Out-To-Out and Out-To-In transitions).The Contractor must provide a Transition-out Strategy outlining how they will design a solution which is able to successfully transition to the next Contract. This Transition-out Strategy must address, at a minimum, the following items:

- proposed knowledge transfer, including:
- records transfer (volumes, formats), including the addressing of data conversion issues;
- approach to how information related to data structures, data domains and data-related processes will be transferred; and
- principles of client transaction history and client account detail migration;
- probable/perceived transition-out Contractor activities;
- timeframes for stopping and queuing procurement processes to export data in the destination system;
- proposed approach to insuring the Contractor will continue the same level and quality of service to clients and stakeholders including continuity of procurement services; and
- proposed approach to incumbent relations including systems consulting file layouts, data fields, explaining codes along with general consulting to explain specific administrative procedures and practices, which are not proprietary.

6.7.1.1 General

Table 116 - Transition Out Roles and Responsibilities

Transition Out Roles and Responsibilities	Contractor	GC
Develop Transition-Out Plan that provides an orderly transition out of the Contractor's service to the future service Contractor.	R	A
The Transition-Out Plan must incorporate appropriate items captured in the Lessons Learned Report from the transition-in implementation. The plan must list all activities, deliverables, dependencies, milestone dates, resource assignments and level of effort, assumptions and the identification of critical dependencies.	R	A
The Transition-Out Plan must address, at a minimum, but not be limited to the following: • transition-out strategy; • project management; • data conversion and migration support; • business change management support; • communications and awareness support; • documentation and file support; • dual service Contractor transition support; • operations support; and • user support.	R	A
Provide the same type and quality of services, under the terms and conditions contained in the Contract, regardless of transactional volume.	R	A

6.7.1.2 OUT-to-OUT Transition Services

Upon the fulfillment of the terms of the associated EPS SOWs for the prescribed Contract durations, or upon termination, it may become necessary for the Contractor to support future in-scope IT service transitions.

This may arise in the event the GC determines that, in lieu of continuing on the existing relationship with the selected Contractor for the provisioning of the in-scope IT services, it would prefer, at its sole discretion, that the provisioning of those services be carried out by another Contractor. In such an event, the Exiting Contractor is expected to support the necessary activities related to transitioning the in-scope IT services to the New Contractor.

Table 117 - Future In-Scope Service Transition Roles and Responsibilities

Future In-Scope Service Transition Roles and Responsibilities	Exiting Contractor	New Contractor	GC
Provide the New Contractor with the lessons learned, assets and documentation from the original transition services provided within the scope of this present SOW.	R	C	A

Future In-Scope Service Transition Roles and Responsibilities	Exiting Contractor	New Contractor	GC
Develop and be primarily responsible for executing a transition plan, and all associated project management and scheduling activities for the affected in-scope IT services, that provides a successful transition of the services from the Exiting Contractor to the New Contractor.	C	R	A
Identify dependencies between the Exiting Contractor and the New Contractor in the context of a transition related to Infrastructure Transition, which includes all activities necessary to transition support of all in-scope systems.	C	R	A
Identify dependencies between the Exiting Contractor and the New Contractor in the context of a transition related to Transition and Migration, which includes ensuring the GC environment is prepared for a transition.	C	R	A
Identify dependencies between the Exiting Contractor and the New Contractor in the context of a transition related to Data Conversion and Migration, which includes the conversion and migration of relevant data.	C	R	A
Identify dependencies between the Exiting Contractor and the New Contractor in the context of a transition related to Transition Integration and Testing, which includes ensuring the right testing plans and requirements are in place to support the testing services necessary for an effective transition.	C	R	A
Identify dependencies between the Exiting Contractor and the New Contractor in the context of a transition related to Organization Change Management & Training Support, which includes thorough technical and End User training, effective communication, and successful stakeholder participation.	C	R	A
Identify dependencies between the Exiting Contractor and the New Contractor in the context of a transition related to Compliance and Regulations, which includes ensuring the EPS is adequately supported by and adherent to related policies, procedures, and regulations.	I	C	R
Perform and support all activities within the future in-scope service transition plan related to Infrastructure Transition, Transition and Migration, Data Conversion and Migration, Transition Integration and Testing, Organization Change Management & Training Support, and Compliance and Regulations for which only the Exiting Contractor can be either directly responsible for, or that are dependent on the Exiting Contractor's support to bring to completion.	R	C	A

6.7.1.3 OUT-to-IN Transition Services from the Contractor to the GC

Upon the fulfillment of the terms of the associated EPS SOWs for the prescribed Contract durations, or upon termination, it may become necessary for the Contractor to support future in-scope IT service transitions from the Contractor to an internal GC entity.

This may arise in the event the GC determines that, in lieu of continuing on the existing relationship with the selected Contractor for the provisioning of the in-scope IT services, it would prefer, at its sole discretion, that the provisioning of those services be carried out internally.

In such an event, the Contractor is expected to support the necessary activities related to transitioning the in-scope IT services to the GC.

Table 118 - Future In-Scope Service Transition from the Contractor to the GC Roles and Responsibilities

Future In-Scope Service Transition from the Contractor to the GC Roles and Responsibilities	Contractor	GC
Provide the GC with the lessons learned, assets and documentation from the original transition services provided within the scope of this present SOW.	R	C
Develop and be primarily responsible for executing a transition plan, and all associated project management and scheduling activities for the affected in-scope IT services, that provides a successful transition of the services from the Contractor to the GC.	C	R
Identify dependencies between the Contractor and the GC in the context of a transition related to Infrastructure Transition, which includes all activities necessary to transition support of all in-scope systems.	C	R
Identify dependencies between the Contractor and the GC in the context of a transition related to Transition and Migration, which includes ensuring the GC environment is prepared for a transition.	C	R
Identify dependencies between the Contractor and the GC in the context of a transition related to Data Conversion and Migration, which includes the conversion and migration of relevant data.	C	R
Identify dependencies between the Contractor and the GC in the context of a transition related to Transition Integration and Testing, which includes ensuring the right testing plans and requirements are in place to support the testing services necessary for an effective transition.	C	R
Identify dependencies between the Contractor and the GC in the context of a transition related to Organization Change Management & Training Support, which includes thorough technical and End User training, effective communication, and successful stakeholder participation.	C	R
Identify dependencies between the Contractor and the GC in the context of a transition related to Compliance and Regulations, which includes ensuring the EPS is adequately supported by and adherent to related policies, procedures, and regulations.	I	R
Perform and support all activities within the future in-scope service transition plan related to Infrastructure Transition, Transition and Migration, Data Conversion and Migration, Transition Integration and Testing, Organization Change Management & Training Support, and Compliance and Regulations for which only the Contractor can be either directly responsible for, or that are dependent on the Contractor's support to bring to completion.	R	C

6.7.1.4 Transition-Out Assets and Documentation

This lists all assets and documentation required in this phase:

- assets (Sole Use and Shared) and Asset Registers;
- asset maintenance history and status;
- subcontracts and associated subcontractor relationships;
- software licenses, including specific references to the software owner's requirements (including transfer);
- status of Third-Party software covering Contractor, version, upgrade status, license and maintenance fees;
- status of custom-developed programs, including source code and documentation;
- customer and other records (including subcontractor agreements that are required to provision the Services);
- configuration information;
- data stored in Contractor or third Party compute environments — including cloud based environments;
- all databases containing GC owned data;
- programs and projects (open and closed ones);
- knowledge databases;
- fault databases;

General documentation, including, but not limited to:

- organization services design and architecture representations;
- software related documentation (user/administrator);
- updated/recent process and procedure documentation;
- workflow and work instruction documentation;
- service management logs - change and incident logs;
- risk register;

Tactical documentation, including but not limited to:

- service-level reports;
- service catalog;
- service delivery plans;
- incident and change register;
- change and project calendar;
- current and scheduled project documents;
- release schedules;
- performance and capacity management planning;
- innovation and service creation plans related to the involved services;
- communication plans and all current and scheduled communication documentation (online and offline);

Strategic documentation, including:

- account plans;
- strategic relationship plans;

- road maps for technology and services;
- enterprise architecture and governance documentation.

6.8 DELIVERABLE SCHEDULE

Table 119 – Deliverable Schedule

SOW Identifier	Deliverable Title	Purpose	Frequency	Timing
3.6.1	Communications Development Principles	The communication plan will be expected to provide a link between business objectives and communications planning and delivery; explain how communications will support the project objectives and which strategic choices have been taken and why; build common understanding of audiences and priorities; create continuity in communications activity over an extended period; articulate objectives and measures of success; and explore and mitigate communications risks.	Once	TBD upon Contract award
3.8.4.6	Table 35 - Performance Management Roles and Responsibilities	Develop and deliver improvement plans as required to meet SLRs based on specified time frame and sequence (e.g., monthly).	As required	TBD upon Contract award
3.8.4.7	Table 36 - IT Life cycle and Operations - Service Delivery: Availability Management	Produce and maintain an Availability Plan which prioritizes and plans approved IT Availability improvements.	Ongoing	TBD upon Contract award
3.8.4.8	Table 37 - IT Life Cycle and Operations - Service delivery: Capacity Management	Develop a quarterly capacity plan.	Quarterly.	Upon Contract Award
3.8.4.10	Table 39 - IT Life Cycle and operations - Service Delivery: Service Continuity & Disaster Recovery	Develop and maintain a detailed DR plan to meet Disaster Recovery requirements. Plan must include plans for data, backups, storage management and contingency operations that provide for recovering GC's systems within established recovery requirement time frames after a disaster affects GC's use of the Services.	Once	TBD upon Contract award

3.8.4.10	Table 39 - IT Life Cycle and operations - Service Delivery: Service Continuity & Disaster Recovery	Develop action plan to address DR testing results.	As required	
3.8.4.12	Table 41 - IT Life Cycle and Operations – Service Delivery: Security	Provide Security plan and IT infrastructure based on Security requirements, standards, procedures, policies, federal, state, and local requirements and risks.	Once	TBD upon Contract award
3.8.4.12	Table 41 - IT Life Cycle and Operations – Service Delivery: Security	Implement physical and logical Security plans consistent with GC Security policies and industry standards in Contractor facilities (e.g., ISO 27001, COBIT).	As required	
3.8.5.1	Table 42 - IT Life Cycle and Operations – Service Support: Change Management	Provide Change Management plan to GC for review.	Once	TBD upon Contract award
3.8.5.3	Table 44 - IT Life Cycle and Operations – Service Support: Release Management	Develop, manage, update and maintain formal Release Management Plans for each Release in coordination with Change Management.	As required	
3.8.5.3	Table 44 - IT Life Cycle and Operations – Service Support: Release Management	Develop quality plans and back-out plans as appropriate for each Release.	As required	
3.8.5.3	Table 44 - IT Life Cycle and Operations – Service Support: Release Management	Provide Release Management Plans and Release Schedules to GC for review.	As required	
3.8.5.5	Table 46 - IT Life Cycle and Operations – Integration and Testing	Develop, document and maintain Integration and Testing procedures and plans that meet requirements and adhere to defined policies.	As required	

3.8.5.6	Table 47 - IT Life Cycle and Operations – Implementation and Migration	Develop, document and maintain Implementation and Migration procedures that meet requirements and adhere to defined policies.	As required	
3.8.5.7	Table 48 - IT Life Cycle and Operations – Training and Knowledge Transfer	Develop, document and maintain Training and Knowledge Transfer procedures that meet requirements and adhere to defined policies.	As required	
3.8.5.7	Table 48 - IT Life Cycle and Operations – Training and Knowledge Transfer	Develop and deliver training program to instruct GC personnel on the provision of Contractor Services (e.g., “rules of engagement,” requesting Services).	Once	TBD upon Contract award
3.8.5.7	Table 48 - IT Life Cycle and Operations – Training and Knowledge Transfer	Develop and implement Knowledge Transfer procedures to ensure that more than one individual understands key components of the business and technical environment.	Once	TBD upon Contract award
3.8.5.9	Table 50 - IT Life Cycle and Operations – Service Support: Incident Management	Develop Incident Management policies, process and procedures that support GC’s Incident Management support requirements.	Once	TBD upon Contract award
3.8.5.10	Table 51 - IT Life Cycle and Operations – Service Support: Problem Management	Develop and implement appropriate process and procedures and methodologies that support GC-approved Problem Management requirements and policies that comply with GC requirements.	Once	TBD upon Contract award
3.8.5.10	Table 51 - IT Life Cycle and Operations – Service Support: Problem Management	Develop and recommend corrective actions or solutions to address recurring incidents and problems, as well as mitigation strategies and actions to take to avert potential problems identified through trend analysis.	As required	
3.8.5.13	Table 54 - IT Life Cycle and Operations – Technology Refreshment and Replenishment	Develop, document and maintain TR&R procedures and develop TR&R plans that meet requirements, adhere to defined policies and Change and Release Management processes.	As required	

3.8.5.13	Table 54 - IT Life Cycle and Operations – Technology Refreshment and Replenishment	Provide management reports on the progress of the TR&R plans.	As required	
3.8.6.13	Table 64 - Application Maintenance	Develop and maintain an Application Maintenance Plan.	As required	
3.8.6.13	Table 64 - Application Maintenance	Provide a comprehensive Disaster Recovery Plan for the System and data in support of GC's requirements.	Once	TBD upon Contract award
6.1	Management and Oversight	The Contractor's Implementation Plan must be used as the basis for reaching the first major Milestone–Delivery of Detailed Final Implementation Plan.	Once	Must submit the final Implementation Plan for Project Authority approval prior to the go-live date.
6.3.4	Three Year Technology Road Map	The Contractor must provide for approval a Technology Road Map during transition and throughout the Contract period to describe how the EPS will be maintained and upgraded over the duration of this Contract.	Updated annually	
6.3.5.1	General	The Contractor must produce and submit to the Project Authority for review, management reports on performance of the project. Management reports must be sufficiently comprehensive to provide "Planned Value" and "Demonstrated Value" comparison reports	Once	TBD upon Contract award
6.4.2	Operational Readiness Plan	The Contractor must submit a draft operational readiness plan within 45 business days after Contract award for approval by GC that identifies a schedule in Microsoft Project format to complete the project plans required in this SOW.	Once	Within 45 business days after Contract award.
6.4.5	Project Management Plan	The Contractor must provide a project management plan	Once	TBD upon Contract award

6.4.6	Overall Transition Plan	The Contractor must submit an overall transition plan for coordinating all activities related to EPS rollout within 30 business days of Contract Award, for approval by GC.	Once	Within 30 business days of Contract Award
6.4.7	Change Management and Communications	The Contractor must provide a change management plan within 60 Business Days of Contract award, for approval by the Project Authority	Once	Within 60 business days of Contract Award
6.4.8	Supplier Enablement Plan	In this section a number of mechanisms, strategies and events are detailed and mapped to the expectations articulated in Part 6.	Once	TBD upon Contract award
6.5.3.4	Table 109 - Transition Planning Roles and Responsibilities	Prepare project plan to support integrated Transition planning and execution.	Once	TBD upon Contract award
6.5.3.4	Table 109 - Transition Planning Roles and Responsibilities	Develop, update, maintain, and revise, a detailed Transition plan(s) that includes approach, activities, milestones, schedule and risk identification and mitigation strategies.	As required	TBD upon Contract award
6.5.3.4	Table 109 - Transition Planning Roles and Responsibilities	Provide status reports and risk mitigation plans weekly.	Weekly	Weekly
6.5.2.6	Table 111 - Transition and Migration Roles and Responsibilities	Develop a thorough implementation readiness assessment plan, readiness assessment schedule, rollback strategy, assessment scorecards, identified and defined critical readiness criteria that will drive go/no-go decisions related to overall readiness/preparedness for going live with any new service or IT environment.	Once	TBD upon Contract award
6.5.3.6	Table 111 - Transition and Migration Roles and Responsibilities	Develop a detailed implementation plan, including a pre-implementation checklist and post-implementation measurable evaluation criteria for the e-Procurement Solution.	Once	TBD upon Contract award
6.5.3.7	Table 112 - Transition Integration and Testing Roles and Responsibilities	Provide proposed integration, test strategy and plan to verify functional, performance, and reliability requirements.	Once	

6.6.1.1	Table 115 - Organizational Change Management & Training Support Roles and Responsibilities	Develop a training plan, material, logistics and schedule	Once	TBD upon Contract award
6.7.1	Contract Phases – Close-out/Transition-out	The Contractor must provide a Transition-out Strategy outlining how they will design a solution which is able to successfully transition to the next Contract.	Once	TBD upon Contract award
6.7.1.1	Table 116 - Transition Out Roles and Responsibilities	Develop Transition-Out Plan that provides an orderly transition out of the Contractor's service to the future service Contractor.	Once	TBD upon Contract award

6.9 DELIVERABLES ACCEPTANCE FRAMEWORK

6.9.1 Definitions

Table 120 - Deliverables Acceptance Framework Key Terms Definition

Term	Definition
Deployment Deliverable	A Deliverable that will be deployed in GC's production systems.
Error Free	Operation without Severity 1, Severity 2 or Severity 3 Incidents.
Major Deliverable	A Deliverable that has the potential to have a significant impact on GC's production systems when implemented.
Minor Deliverable	A Deliverable that is unlikely to have a significant impact on GC's production systems when implemented.

6.9.2 Additional Note on Major and Minor Deliverables

The GC will categorize each of the Deliverables as a Major Deliverable, Minor Deliverable or Deployment Deliverable, and all Deployment Deliverables are considered Major Deliverables.

The GC reserves the right to make subsequent modifications to the classification of the Deliverable as Major Deliverable, Minor Deliverable or Deployment Deliverable.

In the event of any changes to deliverable classification, the GC will need to provide notification of the change in the status to the Contractor.

6.9.3 Deliverables Acceptance Procedures

The GC will provide proposed Acceptance Criteria to the Contractor at least 25 Business Days prior to the date the Contractor must deliver the applicable Deliverable for Major Deliverables, and at least 20 Business Days prior to the applicable Delivery Date for Minor Deliverables.

The amount of time the Contractor may take to review and comment on the Proposed Acceptance Criteria is determined by its nature:

- For Major Deliverables, the Contractor must review and provide detailed comments on the Proposed Acceptance Criteria within 10 Business Days.
- For Minor Deliverables, the Contractor must review and provide detailed comments on the Proposed Acceptance Criteria within 7 Business Days.

The GC reserves the right to determine the final acceptance criteria for each Deliverable. Upon receipt of the Contractor's comments on its proposed Acceptance Criteria, the GC will make any modifications to the proposed criteria it deems reasonable, and provide the final Acceptance Criteria to the Contractor no later than 5 Business Days prior to the Start Date of any Deliverable. The Contractor must review and return its comments, if any, within no more than 3 Business Days of receiving modifications from the GC. Upon receiving the Contractor's additional comments, the GC will make any additional modifications as reasonable, and provide the Final Acceptance Criteria to the Contractor no later than 2 Business Days after receiving the Contractor's comments.

Contractor must submit each Deliverable for Acceptance Testing to the GC on or before the relevant Delivery Date. Prior to submitting the Deliverable for testing, the Contractor must have completed all of the testing (e.g., unit, functional, load, and regression testing) required to be performed by the Contractor with respect to the Deliverable, and will provide the GC with copies and/or summaries of the test results confirming that the Deliverable has passed all such tests.

Upon receiving each Deliverable, the GC will promptly perform acceptance testing in accordance with the applicable Final Acceptance Criteria, and will inform the Contractor of the outcome of such testing:

- Within 15 Business Days for Major Deliverables.
- Within 10 Business Days for Minor Deliverables.

The GC may review the Contractor's interim work products which are produced in the normal course of developing the Deliverable. The GC will notify the Contractor, within a reasonable time period, when the GC would like to informally review these Contractor's interim work products, and provide comments and/or suggestions in a timely manner. The GC may also require the Contractor to provide any additional information it deems necessary, including the identification of the parties responsible for specific testing activities.

6.9.4 Acceptance or Rejection of Deliverables

The GC reserves the right to reject Deliverables that do not meet the agreed upon Acceptance Criteria. At the end of the Acceptance Period, the GC will, in writing either: (1) accept the Deliverable; (2) reject the Deliverable, identifying reasons for rejection; or (3) continue the Acceptance Period in accordance with a mutually-agreed time period for continued review.

In the event that the GC rejects a Deliverable, the Contractor must promptly resolve any outstanding issues that are required in order for the Deliverable to meet all applicable Acceptance Criteria. The

GC will cooperate in the Contractor's efforts to resolve any problems, including indicating the reasons for rejection, and will not unreasonably withhold acceptance.

The GC will give the Contractor timely written notice of acceptance of a Deliverable when, the Deliverable has satisfied the Acceptance Criteria. A Deliverable will be deemed to be accepted by the GC only upon written notice of acceptance.

Following are additional procedures for deployment deliverables:

- Acceptance of all Deployment Deliverables will be subject to a 60 calendar day Error Free period.
- After the expiration of the 60 day Error Free period, if the Deployment Deliverable conforms to the Acceptance Criteria, the GC will accept the Deployment Deliverable.
- In the event that any Deployment Deliverable does not operate Error Free for 60 consecutive calendar days, the GC will reject the Deployment Deliverable and provide the Contractor with a written notice requiring a cure. In response, Contractor must design, develop, and implement a cure, at no additional cost to the GC, and resubmit the Deployment Deliverable for Acceptance in accordance with the section below titled "Re-Submission of a Rejected Deliverable", within 60 calendar days of the written notice.
- If the resubmitted Deployment Deliverable does not conform to the Acceptance Criteria, the GC may (i) immediately terminate the Contract for Cause or (ii) may require the Contractor, at no added cost to the GC, to continue (even beyond this 60 day period) to correct the deficiencies, and to take whatever action is necessary so that the Deployment Deliverable conforms to the Acceptance Criteria. In the case option (ii) above is selected, the GC reserves the right to terminate (as specified in option (i) above) at any time, so long as the Deployment Deliverable is not Accepted.

6.9.5 Re-submission of a Rejected Deliverable

When re-submitting a previously rejected Deliverable, the Contractor must produce a written document that provides a high-level description of how the Deliverable was modified from its previously submitted state, and how this modification will address the concern documented by the GC in the rejection document. Emphasis is to be on establishing conformance with the previously unmet requirements noted in the Deliverable rejection document. This is to both provide assurance that the GC's needs have been met, and to accelerate the Acceptance Period by enabling the GC to focus on reviewing the modifications made by the Contractor.

6.10 SERVICE LEVELS

6.10.1 Client Satisfaction

This service level measures the performance of the service provided to End User or customer used to identify End User's opinion of service performance. The results are used to identify and resolve any issues and problems. Resulting actions should improve End User/management satisfaction.

Table 121 - Client Satisfaction

CLIENT SATISFACTION			
GC Satisfaction	**Service Measure**	**Performance Target**	**SLR Performance %**
Periodic Sample Satisfaction of Acquisitions Program Users	Acquisitions Program Satisfaction Rate	Acquisitions Program Users surveyed should be very satisfied or satisfied	80% (4.0 on a scale of 5.0)
Periodic Sample Satisfaction of GC Users	GC Satisfaction Rate	GC Users surveyed should be very satisfied or satisfied	80% (4.0 on a scale of 5.0)
	Formula	Number of responses with a very satisfied or satisfied rating ÷ total number of responses	
	Measurement Interval	GC Users – Semi-Annually Acquisitions Program Users – Semi-Annually	
	Reporting Period	GC Users – Semi-Annually Acquisitions Program Users – Semi-Annually	
	Measurement Method/Source Data	TBD	

6.10.2 Quality of Delivery

This service level measures at a business function level, the ability of the service Contractor to perform the required services, with a desired result of driving service Contractor behavior toward the reduction of performance errors.

Table 122 - Quality of Delivery

QUALITY OF DELIVERY			
Quality of Delivery	**Service Measure**	**Performance Target**	**SLR Performance %**
Timeliness and correctness of E-Catalog items delivery	Percentage	E-Catalog Users surveyed should indicate that their orders are completed correctly and on time 99% of the time.	99% of the time
	Formula	Number of order fulfillments completed correctly and on time/total number of order fulfillments = service level attained.	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	Tool supplied by service Contractor that automatically records date and time stamps for each activity within a process.	

6.10.3 Problem Management

This service level identifies the effectiveness of Problem Management processes executed by the Contractor, with the objective of improving reducing incident volume over time via proactive trend analysis and identifying permanent fixes to repeated or high-severity incidents.

Table 123 - Problem Management

PROBLEM MANAGEMENT			
Problem Management	**Service Measure**	**Performance Target**	**SLR Performance %**
Incident Reduction Rate	% Reduction	The % reduction of Incidents based over time	Severity One and Two Incidents: -10.00% Severity Three: -15.00% Severity Four: -25.00%
Problem Resolution Rate	Schedule	Total % of Problems resolved via the implementation of permanent fixes within a specified period of time.	Root cause analysis complete: 100% within 2 weeks after creation of Problem record Permanent fix implemented: 90% within 4 weeks after creation of Problem record, or at next available release, whichever is later
	Formula	Incident Reduction: [Total number of Incidents in the Quarter] divided by [Total number of incidents in the corresponding Quarter in the previous year] minus 1] multiplied by 100 = [percentage of Incidents reduction during such quarter]. For the first year of Services, % Reduction is measured from the baseline of Incident volumes established at Transition, subject to review and reset based on Contract Change Management processes. Problem Resolution: [Total number of Problems that are resolved within the target elapsed time] divided by [Total number of Problems] multiplied by 100 = [percentage of Problems resolved in compliance with Problem Resolution Rate performance requirements during such month].	
	Measurement Interval	Incident Reduction: Measure Quarterly Problem Resolution: Measure Monthly	
	Reporting Period	Incident Reduction: Measure Quarterly Problem Resolution: Measure Monthly	
	Measurement Method/Source Data	Measured with ticketing system or by the PMO.	

6.10.4 Change and Release Management

This service level identifies the effectiveness of Change and Release Management processes executed by the Contractor, with the objective of improving stability of the environment via high-quality changes released into production in a scheduled and coordinated manner.

Table 124 - Change and Release Management

CHANGE MANAGEMENT			
Problem Management	**Service Measure**	**Performance Target**	**SLR Performance %**
Defect-Free Changes	Percentage	% of Changes that are implemented with no Defects being determined	98.0%
Release Schedule Adherence	Schedule	% of Changes that are implemented in accordance with the agreed FSR	99.0%
Documentation Timeliness	Elapsed Time	Timeframe for updating documentation and getting GC approval of the updates, in line with the latest Change	1 business day prior to release of the Change
Documentation Quality	Percentage	% of Changes where the related documentation is Accepted by GC to be complete and accurate within the defined Documentation time frames	100%
	Formula	Defect-Free Changes: [Total number of Changes that are not associated with any Defect within the Warranty Period] divided by [Total number of Changes where the Warranty period expires within such month] multiplied by 100 = [percentage of Defect-free Changes during such month]. Release Adherence Schedule: [Total number of Changes that are released in accordance with the schedule in the agreed FSR] divided by [Total number of Changes either contained in the approved FSR within such month] multiplied by 100 = [percentage of Changes released in accordance with the Release Schedule such month].	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

6.10.5 Reporting

This service level identifies the adherence of the Contractor to the agreed schedule and accuracy of reports provided pursuant to the Contract for all services.

Table 125 - Reporting

REPORTING			
Schedule Adherence to Agreed Actions	**Service Measure**	**Performance Target**	**SLR Performance %**
Reporting	Schedule	Provision of reports within the defined time lines in of the Contract	100%
Reporting	Accuracy	% of report data elements that accurately reflect performance, consumption, pricing or status of services	99%
	Formula	Schedule Adherence (%) is based on the number of agreed actions that are completed within the target dates, divided by the total number of agreed actions in the measurement period. Accuracy (%) is based on the number of individual reported data elements that are in line with actuals, divided by the total number of data elements contained in all reports presented within the month.	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Method/Source Data	TBD	

6.11 SERVICE LEVEL FAILURE PENALTIES AND EARN-BACKS

6.11.1 Earn-Back

Following any service level failure, the GC may allow the Contractor the opportunity to earn back the service credits charged in one or more measurement period. If all the service levels for the relevant service and any others agreed to be associated with that service are met, or exceeded, during each of the three measurement periods following the service level failure, the GC may, at its sole discretion, return half of the service credits paid to the Contractor. If all the service levels for the relevant service and any others agreed to be associated with that service are met, or exceeded, during each of the six measurement periods following the service level failure, the GC may, at its sole discretion, return the remaining half of the service credits paid to the Contractor. The Contractor may, where the requisite levels of performance are achieved, make representations to the GC in this regard.

6.11.2 Review of Service Levels

On an as-needed basis after the initial baseline service levels have been established, the GC can request a change to any service level by providing notice to the Contractor that a service level needs to be changed. This change can take effect only after the Contractor has had sufficient time to review the requested change and determine if any modifications are required to the delivery of services.

Should changes be required to the service levels by the Contractor, then the GC must allow the Contractor reasonable time to make such changes before the service level change takes place.

6.11.3 Baseline Service Level Timing

On a quarterly basis beginning six months after the date of signing the Contract, the GC and the Contractor must review the service levels, and agree to adjustments to them or new requirements as appropriate.

PART 7: OPTIONAL SERVICES

7.1 OPTIONAL PROFESSIONAL SERVICES FOR NON-DEFINED WORK

7.1.1 Procurement Advisory Services

The Contractor must provide additional Procurement Advisory Services on an as requested basis. The Contractor must propose expert resources for the provision of the services and their applicable fixed per diem rates. Procurement Advisory Services may include, but are not limited to advisory on:

I. Spend Optimization & Category opportunity identification
II. Complex sourcing and contracting
III. Supplier relationship and risk management
IV. Strategic sourcing
V. Procurement Policy Development
VI. Technology enablement

7.1.2 Additional Change Management and Business Transition Support Services

In addition to the services described in Section 6.5 Transition Services, the Contractor must provide the additional services outlined below to support the transition of procurement operations on an as requested basis.

i. Procurement Process Optimization and Re-engineering
ii. Organizational Change Management
iii. Development of Customized Training
iv. SAP System Architecture and Configuration
v. Master data Architecture

7.1.3 Professional Services Categories

For Work in accordance with the scope of the Contract but that is not otherwise covered by another section of the SOW, the Contractor must provide the professional services outlined below on an as requested basis, during the entire Term of the Contract, including any extensions to it exercised as options by the Contracting Authority in accordance with the Contract. The Work will be requested through an authorized Task Authorization.

A.1 Application/Software Architect
Experience Levels Level 1: < 5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Develop technical architectures, frameworks and strategies, either for an organization or for a major application area, to meet the business and application requirements. • Identify the policies and requirements that drive out a particular solution. • Analyze and evaluate alternative technology solutions to meet business problems. • Ensures the integration of all aspects of technology solutions. • Monitor industry trends to ensure that solutions fit with government and industry directions for technology. • Analyze functional requirements to identify information, procedures and decision flows. • Evaluate existing procedures and methods, identify and document database content, structure, and application sub-systems, and develop data dictionary. • Define and document interfaces of manual to automated operations within application sub-systems, to external systems and between new and existing systems. • Define input/output sources, including detailed plan for technical design phase, and obtain approval of the system proposal. • Identify and document system specific standards relating to programming, documentation and testing, covering program libraries, data dictionaries, naming conventions, etc.

A.6 Programmer/Software Developer
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Develop and prepare diagrammatic plans for solution of business, scientific and technical problems by means of computer systems of significant size and complexity. • Analyze the problems outlined by the systems analysts/designers in terms of such factors as style and extent of information to be transferred to and from storage units, variety of items to be processed, extent of sorting, and format of final printed results. • Select and incorporate available software programs. • Design detailed programs, flow charts, and diagrams indicating mathematical computation and sequence of machine operations necessary to copy and process data and print the results. • Translate detailed flow charts into coded machine instructions and confer with technical personnel in planning programs. • Verify accuracy and completeness of programs by preparing sample data, and testing them by means of system acceptance test runs made by operating personnel. • Correct program errors by revising instructions or altering the sequence of operations. • Test instructions, and assemble specifications, flow charts, diagrams, layouts, programming and operating instructions to document applications for later modification or reference.

A.8 System Analyst
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Develop requirements, feasibility, cost, design, and specification documents for systems. • Implement systems to support projects, departments, organizations or businesses. • Translate business requirements into systems design and specifications. • Analyze and recommend alternatives and options for solutions. • Develop technical specifications for systems development, design and implementation.

A.12 WEB Architect
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Define architecture to be used in web-based projects. • Perform architectural modeling to ensure consistency of the design with existing work. • Select the development language to be used for the project. • Assess the impact of the new requirements on existing web applications. • Develop code based upon design and requirements documents. • Write code to write to and read from the database. • Unit test the code prior to releasing it for integration testing. • Monitor the need for architectural changes as the project progresses. • Develop test plans for testing the system. • Ensure functionalities have been implemented according to specifications. • Define assumptions and constraints of architecture with regard to physical structure and data collection. • Develop post-implementation plan for monitoring/tracking architecture stability.

A.14 WEB Developer
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Develop and prepare diagrammatic plans for web based service delivery over the internet. • Analyze the problems outlined by systems analysts/designers in terms of such factors as style and extent of information to be transferred across the internet. • Select and use the best available web development tools for linking the internet based client to the departmental "back end" information delivery programs and databases. • Design high-usability web pages to meet the requirement. • Verify accuracy and completeness of programs by preparing sample data, and testing them by means of system acceptance test runs made by operating personnel. • Correct program errors by revising instructions or altering the sequence of operations. • Test instructions, and assemble specifications, flow charts, diagrams, layouts, programming and operating instructions to document applications for later modification or reference.

I.1 Data Conversion Specialist
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Oversee all facilities of the conversion process. • Complete mapping, interfaces, mock conversion work, enhancements, actual conversion, and verify completeness and accuracy of converted data. • Establish a strong working relationship with all clients, interact effectively with all levels of client personnel, and provide conversion support. • Analyze and coordinate data file conversions. • Work with importing files from heterogeneous platforms.

I.5 IM Architect
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Analyze existing capabilities and requirements, develop redesigned frameworks and recommend areas for improved capability and integration. Develop and document detailed statements of requirements. • Evaluate existing procedures and methods, identify and document database content, structure, and application subsystems, and develop data dictionary. • Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems. • Prototype potential solutions, provide tradeoff information and suggest recommended courses of action. • Perform information modelling in support of BPR implementation. • Perform cost/benefit analysis of implementing new processes and solutions. • Provide advice in developing and integrating process and information models between business processes to eliminate information and process redundancies. • Provide advice in defining new requirements and opportunities for applying efficient and effective solutions; identify and provide preliminary costs of potential options.

I.11 Technology Architect
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Develop technical architectures, frameworks and strategies, either for an organization or for a major application area, to meet the business and application requirements. • Identify the policies and requirements that drive out a particular solution. • Analyze and evaluate alternative technology solutions to meet business problems. • Ensures the integration of all aspects of technology solutions. • Monitor industry trends to ensure that solutions fit with government and industry directions for technology. • Provide information, direction and support for emerging technologies. • Perform impact analysis of technology changes. • Provide support to applications and/or technical support teams in the proper application of existing infrastructure. • Review application and program design or technical infrastructure design to ensure adherence to standards and to recommend performance improvements.

B.1 Business Analyst
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Develop and document statements for considered alternatives. • Perform business analyses of functional requirements to identify information, procedure, and decision flows. • Evaluate existing procedures and methods, identify and document items such as database content, structure, application subsystems. • Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems. • Establish acceptance test criteria with client. • Support and use the selected departmental methodologies.

B.5 Business Process Re-engineering (BPR) Consultant
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience, or 5+ years of experience with a recognized professional certification
Responsibilities could include but are not limited to: • Review existing work processes and organizational structure. • Analyze business functional requirements to identify information, procedures and decision flows. • Identify candidate processes for re-design; prototype potential solutions, provide trade-off information and suggest a recommended course of action. Identify the modifications to the automated processes. • Provide expert advice in defining new requirements and opportunities for applying efficient and effective solutions; identify and provide preliminary costs of potential options. • Provide expert advice in developing and integrating process and information models between processes to eliminate information and process redundancies. • Identify and recommend new processes and organizational structures. • Provide expert advice on and/or assist in implementing new processes and organizational changes. • Document workflows. • Use business, workflow and organizational modeling software tools.

B.7 Business Transformation Architect
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience, or 5+ years of experience with a recognized professional certification
Responsibilities could include but are not limited to: • Analysis and development of business success "critical success factors". • Analysis and development of architecture requirements design, process development, process mapping and training. • Responsible for leading other functional staff to define business strategy and processes in support of transformation and change management activities. • Participate in change impact analysis and change management activities. • Participate in organizational realignment (job re-design organizational re-structuring). • Coordinate development of training and coordination with other stakeholders. • Create presentations and present to various stakeholders, and facilitate meetings and discussions.

P.1 Change Management Consultant
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience, or 5+ years of experience with a recognized professional certification
Responsibilities could include but are not limited to: • Analysis and development of business "critical success factors". • Analysis and development of architecture requirements design, process development, process mapping and training. • Responsible for leading other functional staff to define business strategy and processes in support of transformation and change management activities. • Participate in change impact analysis and change management activities. • Participate in organizational realignment (job re-design organizational re-structuring). • Coordinate development of training and coordination with other stakeholders. • Create presentations and present to various stakeholders, and facilitate meetings and discussions.

P.4 Organizational Development Consultant

Experience Levels

Level 1: <5 years of experience

Level 2: 5-<10 years of experience

Level 3: 10+ years of experience, or 5+ years of experience with a recognized professional certification

Responsibilities could include but are not limited to:

- Enable, facilitate, and mediate the evolution of the various organizational or departmental structures toward the organization's or department's desired outcome or structure.
- Assist with organizational needs assessment and strategic planning to ensure development of human capital to meet business objectives and goals.
- Provide advice, support and consultation to senior staff, business unit requests, and front line management to achieve strategic initiatives and goals.
- Research, design, implement and maintain employee development programs including leadership development and other management development programs.
- Develop and implement processes to measure the effectiveness of development and learning efforts to ensure performance improvements are focused on measurable and attainable results.
- Serve as an expert resource by collaborating with HR and business unit executives to ensure clear standards and metrics linked to talent reviews and employee development plans.
- Develop strategic partnerships with other internal project managers to identify and consult on change management initiatives to support strategic projects requiring organizational culture change.
- Proactively address and respond to Organizational Development issues by bringing key stakeholders together to assess root causes and performance gaps and recommend appropriate interventions.
- Practice continuous improvement processes and procedures, eliminating non-value added activities.
- Conduct focus groups and/or process improvement sessions as needed.
- Implement and manage the organization's training to ensure cost effective employee development activities that support the organization's strategic initiatives.
- Manage and facilitate organizational initiatives and projects as requested.

C.3 IT Security TRA and C&A Analyst

Experience Levels

Level 1: <5 years of experience
Level 2: 5-<10 years of experience
Level 3: 10+ years of experience

Responsibilities could include but are not limited to:

- Review, analyze, and/or apply Federal, Provincial or Territorial IT Security policies, System IT Security Certification & Accreditation processes, IT Security products, safeguards and best practices, and the IT Security risk mitigation strategies
- Identify threats to, and vulnerabilities of operating systems (such as MS, Unix, Linux, and Novell), and wireless architectures
- Identify personnel, technical, physical, and procedural threats to and vulnerabilities of Federal, Provincial or Territorial IT systems
- Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings
- Conduct Certification activities such as: Develop Security Certification Plans, Verify that security safeguards meet the applicable policies and standards, Validate the security requirements by mapping the system-specific security policy to the functional security requirements, and mapping the security requirements through the various stages of design documents, Verify that security safeguards have been implemented correctly and that assurance requirement have been met. This includes confirming that the system has been properly configured, and establishing that the safeguards meet applicable standards, Conduct security testing and evaluation (ST&E) to determine if the technical safeguards are functioning correctly, Assess the residual risk provided by the risk assessment to determine if it meets an acceptable level of risk
- Conduct Accreditation activities such as: Review of the certification results in the design review documentation by the Accreditation Authority to ensure that the system will operate with an acceptable level of risk and that it will comply with the departmental and system security policies and standards and identify the conditions under which a system is to operate (for approval purposes). This may include the following types of approvals:
- Developmental approval by both the Operational and the Accreditation Authorities to proceed to the next stage in an IT system's life cycle development if sensitive information is to be handled by the system during development
- Operational written approval for the implemented IT system to operate and process sensitive information if the risk of operating the system is deemed acceptable, and if the system is in compliance with applicable security policies and standards
- Interim approval - a temporary written approval to process sensitive information under a set of extenuating circumstances where the risk is not yet acceptable, but there is an operational necessity for the system under development
- Develop and deliver training material relevant to the resource category

C.6 IT Security Engineer

Experience Levels

Level 1: <5 years of experience
Level 2: 5-<10 years of experience
Level 3: 10+ years of experience

Responsibilities could include but are not limited to:

- Review, analyze and/or apply:
  - Directory Standards such as X.400, X.500, and SMTP
  - Operating Systems such as MS, Unix, Linux, and Novell
  - Networking Protocols such as HTTP, FTP, and Telnet
  - Secure IT architectures fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, and SSH
  - IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) stacks
  - Domain Name Services (DNS) and Network Time Protocols (NTP)
  - Network routers, multiplexers and switches
  - Application, host and/or Network hardening and security best practices such as shell scripting, service identification, and access control
  - Intrusion detection/prevention systems, malicious code defence, file integrity, Enterprise Security Management and/or firewalls
  - Wireless technology
  - Cryptographic Algorithms
- Identify the technical threats to, and vulnerabilities of, networks
- Manage the IT Security configuration
- Analyze IT Security tools and techniques
- Analyze the security data and provide advisories and reports
- Analyze IT Security statistics
- Prepare technical reports such as IT Security Solutions option analysis and implementation plans
- Provide Independent Verification and Validation (IV&V) support to IT Security related projects including:
  - IT Security audits, including applicable reports, presentations and other documentation,
  - Review of contingency plans, Business Continuity Plans and Disaster Response Plans
  - Design/development and conduct IT Security protocols tests and exercises
  - Project oversight
- Develop and deliver training material relevant to the resource category

C.7 IT Security Design Specialist

Experience Levels

Level 1: <5 years of experience
Level 2: 5-<10 years of experience
Level 3: 10+ years of experience

Responsibilities could include but are not limited to:

- Review, analyze, and/or apply: Architectural methods, frameworks, and models such as TOGAF, US government FEAP, Canadian government BTEP and GSRM, Zachman, UMM
- Review, analyze, and/or apply a broad range of security technologies including multiple types of systems and applications architectures, and multiple hardware and software platforms, including:
  - Directory Standards such as X.400, X.500, and SMTP
  - Operating Systems such as MS, Unix, Linux, and Novell
  - Networking Protocols (e.g., HTTP, FTP, Telnet)
  - Network routers, multiplexers and switches
  - Domain Name Services (DNS) and Network Time Protocols (NTP)
- Review, analyze, and/or apply Secure IT architectures, standards, communications, and security protocols such as IPSec, SSL, SSH, SMIME, HTTPS
- Review, analyze, and/or apply IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) stacks
- Review, analyze, and/or apply The significance and implications of market and technology trends in order to apply them within architecture roadmaps and solution designs. (examples: web services security, incident management, identity management)
- Review, analyze, and/or apply Best practices and standards related to the concept of network zoning and defence in-depth principles
- Review, analyze, and/or apply IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) stacks
- Analyze IT Security statistics, tools and techniques
- Analyze security data and provide advisories and reports
- Prepare technical reports such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling
- Brief senior managers
- Security architecture design and engineering support
- Conduct data security designation/classification studies
- Prepare tailored IT Security alerts and advisories from open and closed sources Complete tasks directly supporting the departmental IT Security and Cyber Protection Program
- Develop and deliver training material relevant to the resource category

C.8 Network Security Analyst
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
• **Responsibilities could include but are not limited to:** • Review, analyze, and/or apply: o Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH o TCP/IP, UDP, DNS, SMTP, SNMP o Approved GC Cryptographic Algorithms o Directory Standards such as X.400, X.500, and SMTP o Networking Protocols (e.g., HTTP, FTP, Telnet) o Network hardening (for example: shell scripting, service identification) o Technical IT Security safeguards o IT Security tools and techniques o Operating Systems such as MS, Unix, Linux, and Novell o Intrusion detection systems and firewalls o Network routers, multiplexers and switches o Wireless technology • Analyze security data and provide advisories and reports • Conduct impact analysis for new software implementations, major configuration changes and patch management • Develop proof-of-concept models and trials for IT Security • Design/develop IT Security protocols • Identify and analyze technical threats to, and vulnerabilities of, networks • Analyze IT Security tools and techniques • Complete tasks related to authorization and authentication in physical and logical environments • Prepare tailored IT Security alerts and advisories from open and closed sources • Complete tasks directly supporting the departmental IT Security and Cyber Protection Program • Develop and deliver training material relevant to the resource category

C.11 IT Security VA Specialist
Experience Levels Level 1: <5 years of experience Level 2: 5-<10 years of experience Level 3: 10+ years of experience
Responsibilities could include but are not limited to: • Review, analyze, and/or apply: o Threat agents analysis tools and other emerging technologies including privacy enhancement, predictive analysis, VoIP, data visualization and fusion, wireless security devices, PBX and telephony firewall o War dialers, password crackers o Public Domain IT vulnerability advisory services o Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap o Networking Protocols (HTTP, FTP, Telnet) o Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP o Wireless Security o Intrusion detection systems, firewalls and content checkers o Host and network intrusion detection and prevention systems - Anti-virus management • Identify threats to, and technical vulnerabilities of, networks • Conduct on-site reviews and analysis of system security logs • Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses • Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings • Completed tasks directly supporting the departmental IT Security and Cyber Protection Program • Develop and deliver training material relevant to the resource category

7.2 OPTIONAL DEFINED WORK

7.2.1 Additional System Configuration

In accordance with Part 3, GC anticipates the need to modify the solution throughout the operational phase to accommodate changes in the operational environment. While the Statement of Work clearly defines a flexible solution that can be configured by GC administrators, the GC may request additional services in support of changes to the system configuration.

Once EPS is operational, the Contractor must provide additional services, on an as requested basis, to assist in the analysis, design, development, configuration, testing, and roll out of system configurations to the baseline EPS, including but not limited to the following:

i. Workflows
ii. Reports
iii. Templates and Forms
iv. System Fields
v. Localization and Branding

7.2.2 Third Party Integration

In accordance with Part 4, the contractor must deliver, enable and support integration with additional third party systems and data feeds not already articulated in the Statement of Work, on an as requested basis

7.2.3 Tender Feeds

In accordance with Section 5.4, on an as requested basis, the contractor must deliver, enable and support the aggregation, publication, and updating of tender notices including attachments from third party systems and data feeds into the Government Electronic Tendering Service.

7.2.4 Data and Application Escrow

At the request of Canada, the Contractor must ensure a complete copy of GC's EPS updated data set resides in Canada under a data and application escrow agreement. The escrow agreement must be with a named, third party (the escrow agent) who, as a minimum, will be subject to the same CISD security clearances as the Contractor. The data set in escrow must be updated by the Contractor on a daily basis. The data in escrow must be encrypted at rest and in transit to the escrow agent on a secured network. The set of GC's EPS data in escrow must be in a format that is readable by the escrow agent and available to Canada within no later than 1 day of request by Canada.

7.3 OPTIONS FOR OTHER CANADIAN PUBLIC SECTOR ENTITIES

7.3.1 Extending Access to Canadian Public Sector Entities

On an as requested basis, the Contractor agrees to extend access to the GC's EPS instance to any government of any province or municipality in Canada, any Canadian aid agency or public health organization or any intergovernmental organization on an as requested basis.

7.3.2 Option for other Canadian Public Sector Entities to acquire a EPS

The Contractor agrees to extend the provision of the EPS services as defined in the RFP to any government of any province or municipality in Canada, any Canadian aid agency or public health organization or any intergovernmental organization on an as requested basis with substantially the same terms and conditions of the Contract.

ANNEX 2

SECURITY AND PRIVACY

Table of Contents

1.1 SECURITY AND PRIVACY

This Annex provides the security requirements for the e-Procurement Solution (EPS). The components of this document describe to the security requirements for the Solution. Following contract award, the PWGSC Security Assessment and Authorization process will assess how these requirements are addressed.

1.2 OVERVIEW

This document consists of two sections:

1. Section I is a listing of the security requirements which includes a mapping to FedRAMP and CSE guidance (for information purposes only), as well as a mapping to departmental and industry best practices It is expected that the bidder will meet these requirements. The specific mapping of these requirements to FedRAMP and ITSG-33 illustrates how these detailed requirements compare to other security certifications which include but are not limited to FedRAMP, ISO 27001, etc. Throughout the life of the solution, evidence of meeting the requirements will be assessed through the Security Assessment and Authorization process.

2. Section II is a sample of Security Requirements Traceability Matrix.

1.3 BUSINESS CONTEXT SUMMARY

1.3.1 Business Context Summary

The Acquisitions Program is governed by various Acts, Policies and Trade Agreements that need to be taken into consideration while determining the applicable requirements to support the Acquisitions Program and the e-procurement solution. The Solution will be required to have the flexibility to ensure compliance with Canada's procurement regulatory environment, including but not limited to:

- *North American Free Trade Agreement (NAFTA)*
- *Agreement of Internal Trade (AIT)*
- *World Trade Organizational Agreement on Government Procurement (WTO-AGP)*
- *Bilateral Trade Agreements*
- *Comprehensive Land Claims Agreement (CLCA)*
- *TBS Contracting Policy*
- *Canadian International Trade Tribunal (CITT)*
- *Office of the Procurement Ombudsman*
- *Code of Conduct Procurement*
- *Government Contracting Regulations (GCRs)*
- *Financial Administration Act (FAA)*
- *Department of Public Works and Government Services Act*
- *Official Languages Act*
- *Access to Information Act*
- *Canada-European Union: Comprehensive Economic and Trade Agreement (CETA)*

The IT Security Requirements adhere to these governance documents and are suitable for the Acquisitions Program EPS solution as it has been defined to date, as the project progresses some tailoring may have to take place.

Table 1 characterizes in greater detail suitable business contexts using confidentiality, integrity, and availability objectives and examples of consequences of compromise, business processes, and related information. Business activities with such a marking have the following characteristics:

Table 1: Key Business Activities supported by EPS solution

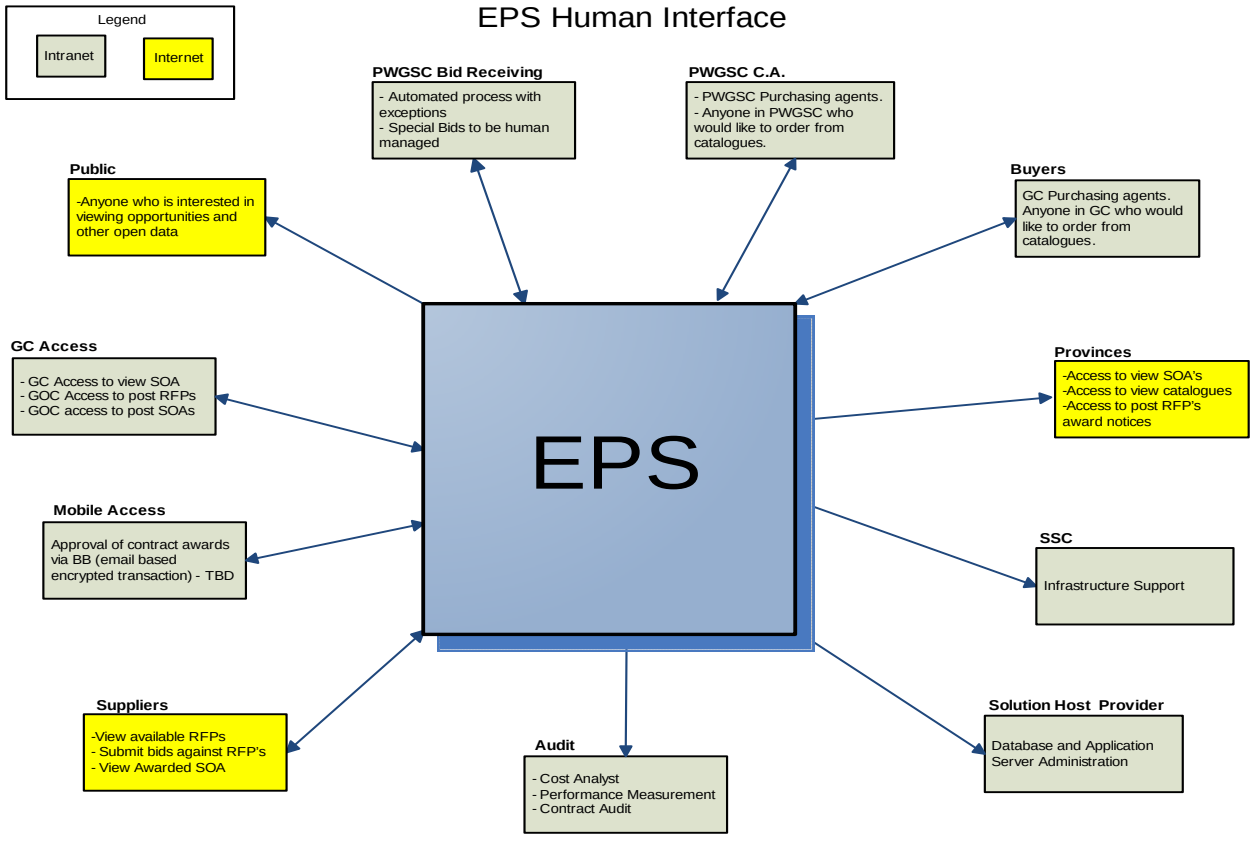
Business Activity	Description
1. Secure access and processing of sensitive procurement information	Acquisitions needs of various groups within the department as well as departments across GC require store, management and processing of sensitive information up to and including **Protected 'B'**. For example: • Client requirements • Supplier information • Bid Information (including potential resumes) • Supplier Financial Information • Contract information – Confidentiality component • Overall Spend information • Trade Secrets
2. Communications and collaboration within the GC and with external organizations	Communications and collaboration with public, Canadian businesses, foreign businesses and partners, provincial and organizations in other countries while maintaining the integrity of the procurement information at all times. For example: • Maintaining the integrity of vendor bids; • Sole-Source Procurement process; • Competitive Procurement process; • Contract Lifecycle Management (CLM) Contract Administration; • Vendor Performance; • Collaboration on Procurement Files – Clients, Buyers, and Suppliers; • Contract Data • Procurement Strategy; • Client Management; • Supplier Management; and • Bid Solicitation process.
3. Ensuring timely availability and delivery of variety of procurement information	Communications and collaboration to enable timely availability of the procurement information to public, vendors, Canadian businesses, foreign business, and partners at provincial, municipal and local levels. For example: • Bid Solicitation – Institutional Access and CPIC clearance • Bid Selection – SRCL Process (supplier facility, personnel, and IT clearance) • Data Center unavailability

Table 1: Key Business Activities supported by EPS solution

Business Activity	Description

1.3.2 Business Use Cases

Figure 1 below provides an overview of the business use cases for the human interfaces associated with the EPS solution.



1.4 TECHNICAL CONTEXT SUMMARY

It is envisioned that EPS is a web-based Software as a Service (SaaS) solution that offers common procurement services for Government of Canada within and outside of the Government of Canada. The EPS shall be built following an N-Tier open architecture pattern and employ Service Oriented Architecture (SOA) for ease of maintenance and interoperability with other systems. The EPS should adhere to the requirements detailed in this Annex which follow industry best practices and ITSG-33 guidelines in

securing its infrastructure, applications and data. The Technology Requirements for the EPS are defined in Section 5.6 (EPS Technology Requirements) in Annex 1- SOW.

While the EPS is expected to be hosted as a Cloud-based solution, Data Segregation of the GC's data is a requirement for EPS. The EPS is also required to securely exchange information with other support systems (both internal and external to GC) and back-office systems already in place, and those that will be introduced in the near future. For example the EPS is expected to play a key role in the GC's Procure-to-pay (P2P) process. While the overall P2P initiative is still in the planning stage, the EPS needs to be part of the overall business flow to support P2P. The EPS also needs to interface with multiple DFMS systems across various Departments. The standard tool for interoperability between GC back office systems and business processes is the Oracle Enterprise Service Bus (ESB). The ESB is currently under development for the GC and is expected to be implemented in time for EPS implementation. For more details on the interoperability requirements for EPS see Section 5.5 (Interfaces with Government of Canada Systems) in Annex 1 – SOW.

The EPS requires a secure access login via GC approved identity, credential and authentication management services in addition to secure access control to the various system components. Section 5.7 (Secure Access) of Annex 1 – SOW provides more information on Secure access in addition to Annex 2.

1.5 THREAT CONTEXT

As indicated in Canada's Cyber Security Strategy,

> *"The evolution of cyber-attack tools and techniques has accelerated dangerously in the recent past. Statistics compiled by two well-known Internet security companies, Akamai and Symantec, together show that malicious computer programs now originate in more than 190 countries. More than 60% of all the malicious code ever detected was introduced into cyberspace in 2008 alone. There is no doubt that the frequency and severity of the cyber threat is accelerating. Protecting Canadians in cyberspace will be a constantly evolving challenge. To effectively address this challenge will require a range of actions and responses, accompanied by continuing investment and vigilance over the long term."*

A Threat assessment is defined in Information Technology Security Guidance (ITSG)-33 as "*the process of identifying and qualifying Threats faced by an organization's business activities and information systems supporting them"*. In order to make informed business and design decisions for the GC Enterprise solutions, a number of threat intelligence reports were consulted.

The ITSG-33 based IT Security Profiles have been developed to protect departmental business activities, the information systems themselves, and the related information processed, stored, and transmitted by those supporting information systems from threats that are relevant to both the business context and the technical context.

Some of the areas of concern to the Acquisitions Program business have been identified from the workshop as:

- Published RFP has been maliciously modified (Integrity);
- Information included within the RFP has been maliciously modified (Integrity);
- Misuse of authorized access and privileges to modify information of evaluated bids (Integrity);
- Inadequate amount of resources internally to clear facilities, personnel, and IT (Availability);
- Unavailability for PWGSC to obtain clearance of suppliers attending mandatory site visits (Availability);
- The reception of bids has been maliciously modified (Integrity);
- Post, issue and amend solicitation (Availability);
- Amendment of tombstone information is maliciously modified;
- The vendor performance data has been maliciously modified;
- Procurement options were incorrectly determined with the clients; and
- The process to accept and reject Statement of Work (SOW), evaluation criteria and bidder selection has been compromised.

In addition to business activities and related information, the information systems themselves (i.e., IT infrastructure) need to be protected from threats, independently of the categorization of the business processes and related information. Many attackers are not interested in GC information or in disrupting GC business activities per se; sometimes they are interested in "setting up shop" by compromising GC information systems to perform illegal acts, such as storing illegal data, images or movies and covertly sharing that data with other criminals; performing denial of service attacks on commercial web sites to extort money, or sending spam.

Threat information has been analyzed from multiple sources, including TBS and departmental threat and incident reports, in addition to CSE's own analysis. As a result, this security control profile, when properly implemented, mitigates the risks from exposure to accidental threats and natural hazards of categories Ta1 to Ta3 and deliberate threat agents of categories from Td1 to Td4, as defined in **Table 2** and **Table 3**, respectively.

While selecting this profile, PWGSC ensured that the threat context is applicable to the Acquisitions Program environment. If there is a change to the threat environment the IT Security requirements may have to be modified to address any threats that would impact the overall security posture of the Acquisitions Program.

Table 2: Applicable Accidental Threat and Natural Hazard Categories

Threat Category	Magnitude of Events
Ta1	Minor accidental events (e.g., trip over a power cord, enter wrong information)
Ta2	• Moderate accidental events (e.g., corrupt database, release information to wrong individual or organization) • Minor hardware or software failures (e.g., hard disk failure) • Minor mechanical failures (e.g., power failure within a section of the facility, temporary power failure) • Minor natural hazards (e.g., localized flooding, earthquake compromising part of the facility)

Table 2: Applicable Accidental Threat and Natural Hazard Categories

Threat Category	Magnitude of Events
Ta3	• Serious inadvertent or accidental events (e.g., cut facility telecommunications or power cables, fire in the facility, large scale compromise of information) • Moderate mechanical failures (e.g., long term facility power failure) • Moderate natural hazards (e.g., localized flooding or earthquake compromising the facility)

Table 3: Applicable Deliberate Threat Categories

Threat Category	Threat Agent Description	Examples of Increasing Threat Agent Capabilities
Td1	Non-malicious adversary (e.g., non-malicious unauthorized browsing, modification, or destruction of information due to the lack of training, concern, or attentiveness.)	• Basic end user capabilities to access information systems and contents.
Td2	Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening, script kiddies).	• Execution of a publicly available vulnerability scanner • Execution of scripts to attack servers • Attempts to randomly delete system files • Modification of configuration files settings
Td3	Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers).	Use of publicly available hacker tools to run various exploits: • Insiders installing Trojans and key loggers on unprotected systems • Use of simple phishing attacks to compromise targets with malware • Execution of programs to crash computers and applications
Td4	Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, and international corporations).	Sophisticated use of publicly available hacker tools • Ability to create own attack tools in software • Basic social engineering attacks • Ability to assemble hardware using COTS components to facilitate attacks • Phishing attacks to gain access to credit card or personal data

1.6 DESCRIPTIONS OF SECURITY POLICY AND PROCEDURE CONTROL CLASSES AND FAMILIES

The following provides a very high level description of the ITSG-33 security control catalogue which is organized into classes and control families. These controls families apply to the EPS security requirements and are addressed by the requirements listed in this Annex. These control families are the basis of securing the application, infrastructure and data.

1.6.1 The technical security class consists of the following control families:

Access control: security controls that support the ability to permit or deny user access to resources within the information system;

Audit and accountability: security controls that support the ability to collect, analyze, and store audit records associated with user operations performed within the information system;

Identification and authentication: security controls that support the unique identification of users and the authentication of these users when attempting to access information system resources; and

System and communications protection: security controls that support the protection of the information system itself as well as communications with and within the information system.

1.6.2 The operational security class consists of the following control families:

Awareness and training: security controls that deal with the education of users with respect to the security of the information system;

Configuration management: security controls that support the management and control of all components of the information system (e.g., hardware, software, and configuration items);

Contingency planning: security controls that support the availability of the information system services in the event of component failure or disaster;

Incident response: security controls that support the detection, response, and reporting of security incidents within the information system;

Maintenance: security controls that support the maintenance of the information system to ensure its ongoing availability;

Media protection: security controls that support the protection of information system media (e.g., disks and tapes) throughout their life cycle;

Physical and environmental protection: security controls that support the control of physical access to an information system as well as the protection of the environmental ancillary equipment (i.e., power, air conditioning and wiring) used to support the operation of the information system;

Personnel security: security controls that support the procedures required to ensure that all personnel who have access to the information system have the required authorizations as well as the appropriate security screening levels; and

System and information integrity: security controls that support the protection of the integrity of the information system components and the data that it processes.

1.6.3 The management security class consists of the following control families:

Security assessment and authorization: security controls that deal with the security assessment and authorization of the information system;

Planning: security controls that deal with security planning activities including privacy impact assessments;

Risk assessment: security controls that deal with the conduct of risk assessments and vulnerability scanning; and

System and services acquisition: security controls that deal with the contracting of products and services required to support the implementation and operation of the information system.

1.7 SECURITY REQUIREMENTS

Table 4 below details an initial set of EPS security requirements. These security requirements might require tailoring as the proposed EPS solution business, technical and security capabilities are better understood and defined through the design and build phases of the EPS implementation in the post contract phase.

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-1	E2.1	Access Control	The Contractor must a) develop, disseminate, and review/update annually, the access control policies and associated access control requirements for e-Procurement Solution Service Infrastructure components; and b) provide PWGSC with the operational security procedures that include operational roles and responsibilities for access control.	AC-1	M
SR-2	E2.2	Access Control	The Identity Credential and Access Management Service must automatically provision Accounts for PWGSC e-Procurement Solution Service User Accounts and Generic Accounts, as follows: a) assign a unique e-Procurement Solution Service Account and Display Name in accordance with the standard defined in subsection , by applying configurable naming and conflict resolution rules; b) create an Account with no privileges; c) assign a one-time temporary password to the Account; d) assign Account attributes and security access privileges **as specified by PWGSC**; and e) return the assigned e-Procurement Solution Service Account, Display Name, **Partner Unique Key, Supplier Unique Key** and one-time password to the Account Requester.	AC-2	M
SR-3	E2.3		The Identity Credential and Access Management Service must a) prevent the re-use of an e-Procurement Solution Service Account as specified by PWGSC; b) allow Account suspension policies as specified by PWGSC;	AC-2	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) not allow access to a suspended Account; d) not allow an Account to send and receive e-Procurement Solution Service work flow messages if the Account is suspended; and e) not allow direct access to the PWGSC e-Procurement Solution Service Solution Service Infrastructure for any Account, as specified by PWGSC.		
SR-4	E2.4	Access Control	The Contractor must manage PWGSC e-Procurement Solution Service Infrastructure Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the PWGSC e-Procurement Solution Service Infrastructure and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) notifying account administrator when temporary accounts are no longer required and when PWGSC e-Procurement Solution Service Infrastructure Operators are terminated, transferred, or PWGSC e-Procurement Solution Service Infrastructure usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year; k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators; iii) accounts after a number of day of inactivity as specified by PWGSC, and iv) temporary and emergency accounts over a given age;	AC-2(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			l) granting access to the e-Procurement Service Infrastructure based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by The Contractor or PWGSC; m) reviewing accounts at least monthly; n) locking the account **after ten (10) unsuccessful login attempts** occurring **within five (5) minutes**, and o) keeping the account locked until manually unlocked by another Operator.		
SR-5	E2.5	Access Control	The PWGSC e-Procurement Solution Service must log the following events: a) Account creation; b) Account modifications c) Account suspension; d) Account termination; e) Account deletion; and f) Account views of e-Procurement Solution Service accounts of which the User is not the primary owner.	AC-2(4)	M
SR-6	E2.6	Access Control	The Contractor must a) define a working hours policy and monitor PWGSC e-Procurement Solution Service Infrastructure Operators accounts utilization against that policy including: i) logging atypical usage of Operator accounts; and ii) alerting designated resources of atypical usage of Operator accounts. b) provide the PWGSC e-Procurement Solution Service Infrastructure Operators accounts atypical utilization log to PWGSC within **one (1) Business Day** of a request by PWGSC; and c) ensure that PWGSC e-Procurement Solution Service Infrastructure Operators log out at the end of their working shift.	AC-2(5)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-10	E2.7	Access Control	The PWGSC e-Procurement Solution Service Infrastructure must enforce access authorizations for Operators.	AC-3	M
SR-11	E2.8	Access Control	The PWGSC e-Procurement Solution Service's Data Loss Prevention (DLP) capability must a) detect violations of data loss prevention policies and apply response actions, as specified by PWGSC, that include: i) blocking transfer of the transaction; ii) blocking transfer of the transaction and return a transaction to the Sender; and iii) other actions agreed to between The Contractor and PWGSC; b) allow real-time enforcement of data loss prevention policies based on the contents of any of the following PWGSC e-Procurement Solution transaction attributes: i) strings, string patterns, and keywords within the transaction body; ii) file type of any attachments; iii) Sender domain; iv) Recipient domain; v) Sender; and vi) Recipient.	AC-4	M
SR-14	E2.9	Access Control	The PWGSC e-Procurement Solution Service must open and scan unencrypted transactions in order to enforce policy against the contents of popular file types as specified by PWGSC.	AC-4(4)	M
SR-15	E2.10	Access Control	The Contractor must implement separation of duties for Operators, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the Operator.	AC-5	M
SR-16	E2.11	Access Control	The Contractor must implement a least privileges policy for PWGSC e-Procurement Solution Service Infrastructure Operators as follows:	AC-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			a) the access control mechanisms must be configured to implement least privilege, allowing only authorized accesses for Operators (and processes acting on their behalf) that are necessary to accomplish assigned tasks; b) create non-privileged accounts to be used for non-operations tasks; c) restrict authorization to super user accounts (e.g., root) to designated Operators; d) restrict sharing of Operator accounts; and e) must uniquely identify the human Operator who has performed each operation on the PWGSC e-Procurement Solution Service Infrastructure.		
SR-17	E2.12	Access Control	The PWGSC e-Procurement Solution Service must automatically lock an Account following a number of unsuccessful login attempts as specified by PWGSC.	AC-7(1)	M
SR-18	E2.13	Access Control	The PWGSC e-Procurement Solution Service must display a logon banner approved by PWGSC on the login page of any web-based application for Users.	AC-8	M
SR-19	E2.14		The PWGSC e-Procurement Solution Service Infrastructure must include an access control mechanism that: a) prevents access to PWGSC e-Procurement Solution Service Infrastructure components or resources without identification, authentication, and authorization; b) displays a PWGSC-approved logon warning banner that authorized operators must acknowledge prior to being granted access to PWGSC e-Procurement Solution Service Infrastructure components; c) notifies the operators, upon successful logon (access), of the date and time of the last logon (access), and d) uses a readily observable logout capability whenever authentication is used to gain access to PWGSC e-Procurement Solution Service Infrastructure components.	AC-8	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-20	E2.15		The PWGSC e-Procurement Solution Service Infrastructure access control mechanisms must include an operator session lock mechanism that: a) prevents further access to Infrastructure components by automatically initiating an operator session lock after a period of inactivity **no longer than 60 minutes**; b) prevents further access to Infrastructure components by initiating an operator session lock when requested by the operators; c) displays a screen saver that contains no meaningful information to completely replace what was previously displayed on the screen upon activation of an operator session lock, and d) unlocks an operator session after successful authentication of the operator.	AC-8	M
SR-21	E2.16	Access Control	The Contractor must ensure that any use of Remote Management within the PWGSC e-Procurement Solution Service Infrastructure take place using a method approved by PWGSC that includes: a)Remote Management must be restricted to PWGSC e-Procurement Solution Service Infrastructure located within a contractor Service Delivery Point using PWGSC e-Procurement Solution dedicated management consoles; b)Documenting allowed methods of Remote Management and establish usage restrictions and implementation guidance for each allowed remote management method; c) monitoring for unauthorized Remote Management; d) authorizing Remote Management prior to connection; e) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods; f) routing all Remote Management to PWGSC e-Procurement Solution Service Infrastructure components through a limited number of managed access control points; g) protecting information about Remote Management mechanisms from unauthorized use and disclosure; and h) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods.	AC-17, AC-17(1), AC-17(3), AC-17(4), AC-17(5), AC-17(6) **ITSG-33 Specific:** AC-17(100)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-23	E2.17	Access Control	The Contractor must not allow wireless access to the PWGSC e-Procurement Solution Service Infrastructure from within the data center facility for privileged users including operators.	AC-18	M
SR-24	E2.18	Access Control	The Contractor must: a) continuously monitor for wireless access points on the PWGSC e-Procurement Solution Service Infrastructure within the Data Center Facility; b) immediately disable any wireless access point when one is discovered, and c) open a security Incident Ticket if a wireless access point is discovered.	AC-18(2)	M
SR-25	E2.19	Access Control	The Contractor must permanently disable all wireless networking functions internally embedded within PWGSC e-Procurement Solution Service Infrastructure.	AC-18(3)	M
SR-26	E2.20	Access Control	The Contractor must not allow a) Mobile Devices to access the PWGSC e-Procurement Solution Service Infrastructure from within the Data Center facility; and b) the use of Mobile Broadband Modems on the PWGSC e-Procurement Solution Service Infrastructure.	AC-19	M
SR-27	E2.21	Access Control	The Contractor must obtain PWGSC's approval for the use of external (i.e., non-Contractor) information systems for the delivery of PWGSC e-Procurement Solution Services.	AC-20	M
SR-28	E2.22	Access Control	The Contractor must limit the use of Contractor-controlled portable storage media within the e-Procurement Solution Service (e.g., thumb drive) as follows: a) restrict the use to authorized Operators only, and b) restrict the use to PWGSC e-Procurement Solution Service Infrastructure components only.	AC-20(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-29	E2.23	Access Control	The Contractor must obtain PWGSC's approval before making any PWGSC e-Procurement Solution Service content publicly available.	AC-22	M
SR-30	E2.24	Security Awareness and Training	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that include operational roles and responsibilities for awareness and training.	AT-1	M
SR-31	E2.25	Security Awareness and Training	The Contractor must provide security awareness and training for PWGSC e-Procurement Solution Service Infrastructure Operators as follows: a) as part of initial training for new Operators; b) before authorizing access to the PWGSC e-Procurement Solution Service Infrastructure or performing assigned duties, and c) annually or when security impacting changes to the e-Procurement Solution Service occur.	AT-2, AT-3	M
SR-32	E2.26	Security Awareness and Training	The Contractor must monitor and document e-Procurement Solution Service security awareness and training for PWGSC e-Procurement Solution Service Infrastructure Operators including: a) documenting who received what training course and when, and b) retaining records for the **last three (3) years**.	AT-4	M
SR-33	E2.27	Audit and Accountability	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that include operational roles and responsibilities for audit and accountability.	AU-1	M
SR-34	E2.28	Audit and Accountability	The e-Procurement Solution Service Identity Credential and Access Management Service must log the following events in accordance with the authentication event logging requirements for Level 3 Assurance, as detailed in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784). a) Successful authentication events; and b) unsuccessful authentication events.	AU-2	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-35	E2.29	Audit and Accountability	The Contractor must a) review and update the list of auditable events for e-Procurement Solution Service at minimum once in **180 Business Days**; b) include execution of privileged functions in the list of audit events; c) log events as identified and approved by PWGSC; and d) automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.	AU-2(3)	M
SR-36	E2.30	Audit and Accountability	The Contractor must ensure that the e-Procurement Solution Service: a) produces audit records that contain sufficient information, **as defined by PWGSC**, to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event; b) or audit events identified by type, location, or subject; and c) manages the content of audit records that are generated.	AU-3	M
SR-37	E2.31	Audit and Accountability	The Contractor must perform capacity management on the e-Procurement Solution Service audit record storage by: a) allocating enough audit record storage capacity; b) configuring auditing to prevent storage capacity being exceeded; c) alerting the Operations Center when the allocated audit record storage volume r**eaches 75% of the audit record storage capacity**; and d) overwriting the oldest audit records if storage reached maximum capacity.	AU-4, AU-5(1)	M
SR-38	E2.32	Audit and Accountability	The PWGSC e-Procurement Solution Service audit function must respond to auditing failures by: a) alerting the Operations Center; and b) overwriting the oldest audit records if storage reached maximum capacity.	AU-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-39	E2.33	Audit and Accountability	The PWGSC e-Procurement Solution Service must use internal system clocks that are synchronized with an authoritative time source, approved by PWGSC, to generate time stamps for audit records.	AU-8, AU-8(1)	M
SR-40	E2.34	Audit and Accountability	The PWGSC e-Procurement Solution Service must: a) protect audit information from unauthorized access, modification, and deletion; and b) backup audit records onto a different system or media than the system being audited on a schedule **as specified by PWGSC**.	AU-9, AU-9(1), AU-9(2), AU-9(3), AU-9(4)	M
SR-41	E2.35	Security Assessment and Authorization	The Contractor must develop an e-Procurement Solution Service vulnerability mitigation plan approved by PWGSC **within five (5) Business Days** of completion of a vulnerability assessment that includes proposed protection measures to mitigate the risks identified from the vulnerability assessment.	CA-7(2)	M
SR-42	E2.36	Configuration Management	The Contractor must develop, document, and maintain under configuration control, a current baseline configuration of the PWGSC e-Procurement Solution Service Infrastructure components and the **two (2) previous versions**.	CM-2, CM-2(1), CM-2(2), CM-2(3), CM-2(4)	M
SR-43	E2.37	Configuration Management	The Contractor must only allow authorized software, as documented by the Contractor and approved by PWGSC, to execute on the PWGSC e-Procurement Solution Service.	CM-2(5)	M
SR-44	E2.38	Configuration Management	The Contractor must a) plan, test the implementation of new and changed software, hardware and documentation for a PWGSC e-Procurement Solution Service release not using the production environment or the control test environment of the PWGSC e-Procurement Solution Services;	CM-3(2), CM-3(3), CM-3(4)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			b) implement new and changed software, hardware and documentation for a PWGSC e-Procurement Solution Service release as approved by PWGSC; and c) develop and implement procedures for the distribution, installation, and rollback of changes implemented for a PWGSC e-Procurement Solution Service release.		
SR-45	E2.39	Configuration Management	The Contractor must assess the security impact of changes by: a) analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; b) informing PWGSC of potential security impacts prior to change implementation, and c) checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements.	CM-4	M
SR-46	E2.40		The Contractor must conduct audits of information system changes **at least every 12 months** and when indications so warrant determining whether unauthorized changes have occurred.	CM-4	M
SR-47	E2.41	Configuration Management	The Contractor must review PWGSC e-Procurement Solution Service infrastructure Operator privileges on an annual basis.	CM-5(5)	M
SR-48	E2.42	Configuration Management	The Contractor must manage configuration settings for PWGSC e-Procurement Solution Service Infrastructure that includes: a) specifying configuration settings to implement least privilege/functionality; b) documenting exceptions to configuration settings; and c) monitoring and controlling changes to the configuration settings in accordance with the Change Management and Configuration Management processes.	CM-5(7)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-49	E2.43	Configuration Management	The Contractor must employ automated mechanisms to centrally manage, apply, and verify configuration settings and to respond to unauthorized configuration changes by creating a Security Incident Ticket.	CM-6, CM-6(1), CM-6(2)	M
SR-50	E2.44	Configuration Management	The Contractor must open a security Incident Ticket when an unauthorized configuration change is detected in the e-Procurement Solution Service.	CM-6(3)	M
SR-51	E2.45	Configuration Management	The Contractor must configure the PWGSC e-Procurement Solution Service to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services **as approved by PWGSC**.	CM-7, CM-7(1), CM-7(2), CM-7(3)	M
SR-52	E2.46	Configuration Management	The Contractor must develop, document, and maintain an inventory of the PWGSC e-Procurement Solution Service components that: a) accurately reflects their current configuration; b) is at the level of granularity deemed necessary for tracking and reporting; c) includes enough information to achieve effective property accountability; d) is available for review and audit by PWGSC; and e) is updated as an integral part of component installations, removals, and PWGSC e-Procurement Solution Service updates.	CM-8, CM-8(1)	M
SR-53	E2.47	Configuration Management	The Contractor must provide PWGSC with a change management process that includes measures used to enforce only authorized changes as applicable to the e-Procurement Solution Service.	CM-8(2), CM-8(3), CM-8(4), Cm-8(5), CM-8(6)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-54	E2.48		The Contractor must employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of PWGSC e-Procurement Solution Service Infrastructure components that: a) detect the addition of unauthorized components into the PWGSC e-Procurement Solution Service Infrastructure, and b) create a Security Incident Ticket.	CM-8(2), CM-8(3), CM-8(4), Cm-8(5), CM-8(6)	M
SR-55	E2.49	Configuration Management	The Contractor must provide a e-Procurement Solution Service Configuration Management Plan that: a) addresses roles, responsibilities, and configuration management processes and procedures; b) defines the Configuration Items for PWGSC e-Procurement Solution Services and when the Configuration Items are placed under configuration management; c) establishes the means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items; d) defines the processes for patch management on custom software utilized within the PWGSC e-Procurement Solution Service Infrastructure that includes: i) identifying, reporting, and correcting flaws in custom software; ii) testing software updates related to flaw remediation for effectiveness and potential side effects on the e-Procurement Solution Service before installation; iii) incorporating flaw remediation into the e-Procurement Solution Service configuration management process; e) defines the processes for patch management of the PWGSC e-Procurement Solution Service Infrastructure components that includes: i) ensuring the latest version of applications and operating systems are used; ii) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; iii) prioritizing critical patches using a risk-based approach; iv) taking applications offline and bringing them back online;	CM-9, CM-9(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			v) aligning criticality levels for patches as specified by PWGSC; vi) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; vii) testing and verification methodology to ensure that patches have been implemented properly; and viii) notifying PWGSC of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of PWGSC e-Procurement Solution Service.		
SR-56	E2.50		The Contractor must provide PWGSC with a e-Procurement Solution Service change management process that includes: a) Contractor's change management authorities; b) Contractor resource roles and responsibilities for change management; c) how The Contractor will use the change management process to support the development of the PWGSC e-Procurement Solution Services (e.g., a concept of operation); d) method used to uniquely identify configuration items; e) configuration item identification method; f) means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items;	CM-9, CM-9(1)	M
SR-57	E2.51	Contingency Planning	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that include operational roles and responsibilities for contingency planning.	CP-1, CP-2	M
SR-58	E2.52	Contingency Planning	The Contractor must coordinate the development and testing of the Service Continuity Plan with the organizational groups, within the Contractor and PWGSC, responsible for related plans.	CP-2(1), CP-2(2), CP-2(3), CP-2(4), CP-2(5), CP-2(6)	M
SR-59	E2.53		The Contractor must conduct capacity planning so that necessary capacity for e-Procurement Solution Service processing, telecommunications, and environmental support exists during contingency operations.	CP-2(1), CP-2(2), CP-2(3),	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
				CP-2(4), CP-2(5), CP-2(6)	
SR-60	E2.54		The Contractor must train its personnel in their contingency roles and responsibilities with respect to the e-Procurement Solution Service, including simulated events to facilitate effective response in crisis situations, and provide refresher training at least annually.	CP-2(1), CP-2(2), CP-2(3), CP-2(4), CP-2(5), CP-2(6)	M
SR-61	E2.55	Contingency Planning	The Contractor must work in conjunction with PWGSC to establish national restoration priorities for PWGSC e-Procurement Solution Services in an order of precedence **as specified by PWGSC.**	CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-7(5), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4)	M
SR-62	E2.56	Contingency Planning	The Contractor must a) test the backup data for PWGSC e-Procurement Solution Services monthly to verify media reliability and data integrity; and b) use a sample of backup data for PWGSC e-Procurement Solution Services in the restoration of selected PWGSC e-Procurement Solution Service functions as part of service continuity plan testing.	CP-9, CP-9(1), CP-9(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-63	E2.57	Contingency Planning	The Contractor must store backup copies of operating system software, critical system software, and component inventory in a separate facility or fire-rated container that is not collocated with the PWGSC e-Procurement Solution Service Infrastructure.	CP-9(3)	M
SR-64	E2.58	Contingency Planning	The Contractor must transfer any e-Procurement Solution Service backup data **within 24 hours of the backup being done to an alternate storage site.**	CP-9(5)	M
SR-65	E2.59	Contingency Planning	The Contractor must restore the PWGSC e-Procurement Solution Services to a known state after a disruption, compromise, or failure.	CP-10	M
SR-66	E2.60	Contingency Planning	The Contractor must refresh the disk images of PWGSC e-Procurement Solution Service components from configuration-controlled and integrity-protected disk images.	CP-10(4)	M
SR-67	E2.61	Identification and Authentication	The Contractor must provide PWGSC with the operational security procedures that includes operational roles and responsibilities for identification and authentication requirements specified in this SOW.	IA-1	M
SR-68	E2.62	Identification and Authentication	The PWGSC e-Procurement Solution Service must a) uniquely identify and authenticate Operators (or processes acting on behalf of Operators). b) issue user name and password credentials for Accounts that comply with the requirements for **Level 2 Assurance** as described in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784). c) allow challenge/response questions for password recovery; d) allow one-time temporary passwords for enrolment and password recovery; e) allow one-time temporary passwords must be subject to a configurable validity period, as specified by PWGSC; f) allow one-time temporary passwords must be sufficiently random so as to not be predictable as approved by PWGSC; g) allow automatic advanced notification of pending password expiry as specified by PWGSC;	IA-2	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			h) allow password recovery policies and processes; and i) authenticate all Software Client access to the PWGSC e-Procurement Solution Service.		
SR-69	E2.63	Identification and Authentication	The PWGSC e-Procurement Solution Service Identity Credential and Access Management Service must allow the binding and un-binding of one or more credentials to an individual Account. (e.g., an individual could use their PWGSC e-Procurement Solution **Level 2 credential** to access the PWGSC e-Procurement Solution Service as a User and use an additional X.509 credential to access the PWGSC e-Procurement Solution Service for administrative functions.).	IA-2(1)	M
SR-70	E2.64	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must a) enforce two-factor authentication using hard crypto token for all Operator accounts in compliance with CSE ITSG-31(https://www.cse-cst.gc.ca/en/node/267/html/22784); and b) perform mutual authentication of Operators Portable Devices connected to the network and only accept authorized Operators Portable Devices.	IA-3, IA-3(1), **CSE ITSG-33 Specific:** IA-2(100)	M
SR-72	E2.65	Identification and Authentication	The Contractor must manage PWGSC e-Procurement Solution Service Infrastructure Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the PWGSC e-Procurement Solution Service Infrastructure and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;	IA-4	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			i) notifying account administrator when temporary accounts are no longer required and when PWGSC e-Procurement Solution Service Infrastructure Operators are terminated, transferred, or PWGSC e-Procurement Solution Service Infrastructure usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year; k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators; iii) accounts after a number of day of inactivity as specified by PWGSC, and iv) temporary and emergency accounts over a given age; l) granting access to the PWGSC e-Procurement Solution Service Infrastructure based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by The Contractor or PWGSC; m) reviewing accounts at least monthly; n) locking the account after 10 unsuccessful login attempts occurring within 5 minutes, and o) keeping the account locked until manually unlocked by another Operator.		
SR-73	E2.66		The PWGSC e-Procurement Solution Service Identification Credential and Access Management service must log the following events: a) account creation; b) account modifications c) account disabling, d) account termination; e) for Level 3 Assurance, as detailed in ITSG-31: i) password changes; ii) credential registrations; iii) password recovery;	AU-2(3), IA-4	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			iv) expired credentials		
SR-74	E2.67		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible.	AU-2(3), IA-4	M
SR-75	E2.68	Identification and Authentication	The PWGSC e-Procurement Solution Service Identity Credential and Access Management Service must automatically provision 1) Accounts for User e-Procurement Accounts and Generic Accounts, as follows: a) assign a unique e-Procurement Account and Display Name in accordance with the standard defined in subsection , by applying configurable naming and conflict resolution rules; b) create an Account with no privileges; c) assign a one-time temporary password to the Account; d) create a Mailbox for the Account (if necessary); e) assign Account attributes and security access privileges as specified by PWGSC; and f) return the assigned e-Procurement Email Address, Display Name, Partner Unique Key, Contractor Unique Key and one-time password to the Account Requester.	IA-4(1)	M
SR-76	E2.69	Identification and Authentication	The Contractor designated registration authority must provide e-Procurement Solution Service Operator identifiers and authenticators (e.g., username, password, cryptographic token, etc.) in person to the authorized Operator.	IA-4(2)	M
SR-77	E2.70	Identification and Authentication	The Contractor must require multiple forms of physical identification be presented by an Operator for PWGSC e-Procurement Solution Services to a Contractor registration authority before the Operator receives identifiers and authenticators to access the PWGSC e-Procurement Solution Service Infrastructure.	IA-4(3)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-78	E2.71	Identification and Authentication	The Contractor must manage user authenticators for Operators by: a) verifying, as part of the initial authenticator distribution, the identity of the individual receiving the authenticator; b) establishing initial authenticator content for authenticators defined by the Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon PWGSC e-Procurement Solution Service Infrastructure component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing/refreshing authenticators at a frequency not exceeding 180 days; h) protecting authenticator content from unauthorized disclosure and modification, and i) requiring Operators to take specific measures to safeguard authenticators.	IA-5	M
SR-79	E2.72		The Contractor must manage device authenticators by: a) verifying, as part of the initial authenticator distribution, the identity of the device receiving the authenticator; b) establishing initial authenticator content for authenticators defined by The Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon PWGSC e-Procurement Solution Service Infrastructure component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing/refreshing authenticators at a frequency not exceeding 180 days; h) protecting authenticator content from unauthorized disclosure and modification, and i) having devices implement specific measures to safeguard authenticators.	IA-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-80	E2.73		The PWGSC e-Procurement Solution Service authentication process for X.509 credentials must include: a) performing path validation of the X.509 certificate; and b) checking the revocation status of the X.509 certificate.	IA-5	M
SR-81	E2.74	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must, for password-based authentication: a) enforce minimum password complexity of **case sensitive, 15 characters, with at least one upper case, one lower case, one number, and one special character**; b) encrypt passwords in storage and in transmission; c) enforce password **maximum lifetime of 90 days**, and d) prohibit password **reuse for 10 generations**.	IA-5(1)	M
SR-82	E2.75		The PWGSC e-Procurement Solution Service Identity Credential and Access Management Service must provide a) the User with a checklist that presents the rules a password must comply with and check these rules positively as they are satisfied when the User enters the password. b) configurable User password rules as specified by PWGSC that include: i) minimum number of total characters; ii) minimum number of uppercase and lowercase characters; ii) minimum number of numeric characters; iv) minimum number of non-alpha-numeric characters; v) words found in dictionary (English and French); vi) password re-use history; vii) maximum lifetime of the password.	IA-5(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-83	E2.76	Identification and Authentication	The Contractor must require that the registration process for PWGSC e-Procurement Solution Service Operators to receiver identifiers and authenticators be carried out in person before a designated registration authority with authorization by a designated Contractor's official (e.g., a supervisor).	IA-5(3)	M
SR-84	E2.77	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must not transmit clear text passwords over any network.	IA-5(6)	M
SR-85	E2.78	Identification and Authentication	The Contractor must not allow unencrypted static authenticators to be embedded in PWGSC e-Procurement Solution Service Infrastructure applications or access scripts or stored on function keys.	IA-5(7)	M
SR-86	E2.79	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must obscure feedback of Operator authentication data (e.g., masking password fields) during the authentication process.	IA-6	M
SR-87	E2.80	Identification and Authentication	The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the PWGSC e-Procurement Service have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.	IA-8	M
SR-88	E2.81	Incident Response	1) The Contractor must provide PWGSC with the operational security procedures that includes operational roles and responsibilities for Incident response requirements specified in this SOW.	IR-1	M
SR-89	E2.82		The Contractor must implement and test the service continuity plan (all processes, procedures, roles, responsibilities etc) on an annual basis, and provide the test results to PWGSC within 10 Federal Government Working Days of completion of the service continuity plan testing.	IR-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-90	E2.83		The Contractor must provide a service continuity plan (SCP) to PWGSC that includes: a) detailed plan and documented processes for restoring PWGSC e-Procurement Solution Services; b) details the communications plan with PWGSC and its suppliers; c) details plan and processes for transferring operational, management and administration functionality to a backup operations centre; d) back up strategies for datacenter facilities, network facilities, operational support systems and data, and key service components; e) how The Contractor will ensure that its suppliers have in place service continuity plans; f) describes the process for testing the Service Continuity Plan; g) steps The Contractor will take if any of its key suppliers go out of business, and h) steps The Contractor will take if any of its manufacturers or Original Equipment Manufacturers (OEM) is no longer considered a trusted manufacturer or OEM by PWGSC.	IR-1	M
SR-91	E2.84		The Contractor must provide a final version of the Service Continuity Plan within 15 Federal Government Working Days after receiving comments from PWGSC on the draft Service Continuity Plan.	IR-1	M
SR-92	E2.85		The Contractor must implement the Service Continuity Plan (all processes, procedures, roles, responsibilities etc.), and any subsequent annual updates, within 60 Federal Government Working Days following acceptance by PWGSC.	IR-1	M
SR-93	E2.86		The Contractor must provide to PWGSC within 40 Federal Government Working Days of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the Service Continuity Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting PWGSC's service continuity requirements.	IR-1	M
SR-94	E2.87		If The Contractor determines that it will take more than 40 Federal Government Working Days to provide the requested evidence for the Service Continuity Plan, The Contractor must notify PWGSC within 5 Federal Government Working Days of the original request for evidence, and request an extension, in writing with appropriate justification. Granting an extension is within PWGSC's sole discretion.	IR-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-95	E2.88		The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance.	IR-1	M
SR-96	E2.89		In addition to any sources of intelligence on cyber threats and Incidents sources that The Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).	IR-1	M
SR-97	E2.90		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.	IR-1	M
SR-98	E2.91		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.	IR-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-99	E2.92		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) security Incident handling and response; and d) auditing.	IR-1	M
SR-100	E2.93		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.	IR-1	M
SR-101	E2.94		The Contractor must automatically provide Incident Ticket information by secure e-mail to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).	IR-1	M
SR-102	E2.95		The Contractor must continue to automatically send secure e-mail upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-1	M
SR-104	E2.96		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-1	M
SR-105	E2.97		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number;	IR-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.		
SR-106	E2.98		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible	IR-1	M
SR-107	E2.99		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.	IR-1	M
SR-108	E2.100	Incident Response	The Contractor must provide training for PWGSC e-Procurement Solution Service Infrastructure Operators in their security Incident response roles and responsibilities and provide annual refresher training.	IR-2	M
SR-109	E2.101		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies:	IR-2	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).		
SR-110	E2.102		The Contractor must continue to automatically send e-Procurement upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-2	M
SR-112	E2.103		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-2	M
SR-113	E2.104		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.	IR-2	M
SR-114	E2.105		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible.	IR-2	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-115	E2.106		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.	IR-2	M
SR-116	E2.107	Incident Response	The Contractor must test the Incident response process for the e-Procurement Solution Service at least annually using comprehensive test scripts to determine the Incident response effectiveness including: a) documenting the test results; b) reviewing the test results with PWGSC, and c) implement corrective actions as required by PWGSC within a timeframe agreed to with PWGSC.	IR-3	M
SR-117	E2.108	Incident Response	The Contractor must ensure that the security posture of the PWGSC e-Procurement Solution Services is maintained by continuously: a) monitoring threats and vulnerabilities; b) monitoring for malicious activities and unauthorized access; and c) where required, taking proactive countermeasures, including taking both pre-emptive and response actions to mitigate threats.	IR-4	M
SR-118	E2.109		The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and	IR-4	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance.		
SR-119	E2.110		In addition to any sources of intelligence on cyber threats and Incidents sources that the Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).	IR-4	M
SR-120	E2.111		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.	IR-4	M
SR-121	E2.112		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.	IR-4	M
SR-122	E2.113		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.	IR-4	M
SR-123	E2.114		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and	IR-4	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			b) allowing PWGSC to provide on-site guidance and coordination. (The SOC must use a Secure Terminal Equipment (STE), provided as Government Furnished Equipment, following existing COMSEC processes, to communicate with PWGSC when requested by PWGSC that includes a unique and dedicated telephone number.		
SR-124	E2.115		The SOC must accept e-mails from PWGSC authorized representatives to a Contractor-provided mailbox with an auto reply to confirm receipt of the e-mail.	IR-4	M
SR-125	E2.116		The SOC must acknowledge receipt of e-Procurements received from e-Procurement addresses authorized by PWGSC **within 15 minutes** of receiving the e-Procurement 24 hours per day, 7 days per week, and 365 days per year.	IR-4	M
SR-126	E2.117		The SOC must authenticate the identity of the requester using a process approved by PWGSC	IR-4	M
SR-127	E2.118		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).	IR-4	M
SR-128	E2.119		The Contractor must continue to automatically send e-mail upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-4	M
SR-130	E2.120		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-4	M
SR-131	E2.121		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number;	IR-4	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.		
SR-132	E2.122		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible	IR-4	M
SR-133	E2.123		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.	IR-4	M
SR-134	E2.124		The Contractor must create one or more Incident Tickets for each Incident detected by The Contractor or reported by PWGSC.	IR-4	M
SR-135	E2.125		The Contractor must physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in PWGSC dedicated storage.	IR-4	M
SR-136	E2.126		The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and PWGSC-reported Incidents.	IR-4	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-137	E2.127		The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.	IR-4	M
SR-138	E2.128	Incident Response	The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements files) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-4(2)	M
SR-139	E2.129		The Contractor must create an Emergency Change Request, within a time period specified by PWGSC, for each mitigation measure requested by PWGSC to contain a Security Incident.	IR-4(2)	M
SR-140	E2.130		The Contractor must create an Emergency Change Request, based on severity as specified by PWGSC, for each mitigation measure requested by PWGSC to contain a Security Incident and, must implement the Emergency Change Request in accordance with PWGSC's priority level.	IR-4(2)	M
SR-141	E2.131	Incident Response	The Contractor must a) revise the severity level and priority of an Incident when requested to do so by PWGSC within 15 minutes of the request; b) automatically escalate Incidents according to escalation levels and time periods specified by PWGSC; c) provide PWGSC with an operational escalation matrix and a management escalation matrix that defines the personnel, with alternates (of equal authority) for a minimum of 5 Escalation Levels (Escalation Level 1 to Escalation Level 5, where Escalation Level 5 is the most senior personnel), and contains clear contact instructions; d) provide PWGSC with notification of Incidents according to the operational and management escalation matrices; and e) classify, assign and escalate Incidents for Incident resolution based on priority in accordance with severity and impact levels as specified by PWGSC.	IR-4(3)	M
SR-142	E2.132	Incident Response	The Incident Tickets for Security Incidents must include, the following additional information: a) type and description of attack/event; b) whether attack appears to have been successful and impact; c) attack scope (to an organization and/or across many organizations);	IR-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			d) estimated number of systems affected by organization; e) list of systems affected by organization; f) apparent source/origin of attack/Incident/event; g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration; k) actions taken; l) status of mitigations, and m) applicable logs or evidence data.		
SR-143	E2.133		The Contractor must automatically provide Incident Ticket information by Email to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).	IR-5	M
SR-144	E2.134		The Contractor must continue to automatically send Email upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-5	M
SR-146	E2.135		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-5	M
SR-147	E2.136		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date;	IR-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.		
SR-148	E2.137		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible.	IR-5	M
SR-149	E2.138		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service. The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.	IR-5	M
SR-150	E2.139		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller;	IR-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.		
SR-151	E2.140		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.	IR-5	M
SR-152	E2.141		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.	IR-5	M
SR-153	E2.142	Incident Response	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance.	IR-6	M
SR-154	E2.143		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.	IR-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-155	E2.144		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.	IR-6	M
SR-156	E2.145		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.	IR-6	M
SR-157	E2.146		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.	IR-6	M
SR-158	E2.147		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).	IR-6	M
SR-159	E2.148		The Contractor must continue to automatically send e-Procurement upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-160	E2.149		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-6	M
SR-161	E2.150		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible	IR-6	M
SR-162	E2.151		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.	IR-6	M
SR-163	E2.152		Add these items to the Security Incident Ticket: g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration;	IR-6	M
SR-164	E2.153		The Contractor must report all suspected or actual privacy and security violations for PWGSC e-Procurement Solution Services as Security Incidents.	IR-6	M
SR-165	E2.154		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates;	IR-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).		
SR-166	E2.155		The Contractor must provide all evidence, in a COTS format specified by PWGSC, associated to a Security Incident, within a time interval specified by PWGSC that includes: a) results of historical logs and audit records research associated with one or many Partners based on criteria provided by PWGSC; b) results of analysis of logs and audit records associated with one or many organizations based on criteria provided by PWGSC; c) logs and audit records based on criteria provided by PWGSC, and d) additional information or data as specified by PWGSC.	IR-6	M
SR-167	E2.156		The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and PWGSC-reported Incidents.	IR-6	M
SR-168	E2.157		The Contractor must update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.	IR-6	M
SR-169	E2.158		The Contractor's Incident Tickets must include and maintain, but not be limited to, the following dedicated information fields for all Incidents: a) Contractor's Ticket number; b) Incident description; c) Incident originator contact information (name, telephone number and e-Procurement address); d) Incident originator language; e) related Incident Tickets; f) date and time stamp when Incident Tickets initiated; g) date and time stamp when Incident Ticket closed; h) Incident Ticket type; type (e.g. production, functional testing, performance testing, security, etc.) as specified by PWGSC; i) Incident Ticket severity; j) Incident Ticket impact;	IR-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			k) Incident Ticket priority; l) Incident Ticket status (i.e. open, closed, in progress, suspended, cancelled etc.); m) Incident Ticket escalations;<TRACEFROM>SR-599</TRACEFROM> n) PWGSC's ticket number; o) Service functions impacted; p) affected Service Delivery Points; q) Contractor contact (name, telephone number and e-Procurement address); r) Partner identifier (If applicable); s) Interactions with third parties;<TRACEFROM>SR-599</TRACEFROM> t) activity log; u) root cause (if available); v) estimated time for resolution (updated every 15 minutes); w) resolution description and x) outage time (for closed tickets only).		
SR-170	E2.159		The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and PWGSC-reported Incidents.	IR-6	M
SR-171	E2.160		The Contractor must update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.	IR-6	M
SR-172	E2.161		The Contractor must notify PWGSC via phone and e-Procurement (7 days x 24 hours x 365 days), based on priority as specified by PWGSC, of any suspected or actual Security Incidents, including: ii) denial of service attacks; iii) malware; iv) social engineering; v) unauthorized intrusion or access; vi) information breach; and vii) all other security breaches or cyber threats targeting Canada.	IR-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-173	E2.162		The Contractor must not withhold from PWGSC any information or data in its possession that relates to PWGSC e-Procurement Solution or is associated with a Security Incident.	IR-6	M
SR-174	E2.163		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.	IR-6	M
SR-175	E2.164		The Contractor must provide a secure Security Management Portal that will allow Canada to view security-related information within the PWGSC e-Procurement Solution Service. This includes but is not limited to: a) security Incident reports, post-mortem, adhoc reports, and associated evidence; b) security Incident tickets; c) user activity reports; d) operator activity reports; e) access reports; f) configuration audit reports; g) configuration change reports; h) file integrity monitoring reports; i) inventory reports; j) vulnerability reports;	IR-6	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			k) configuration change reports; l) Emergency Request For Changes and Request For Changes; m) patches and security patches implemented; n) information on whether specific e-Procurements are being blocked/filtered and for how long; and o) other supporting documentation (e.g. whitelisting, blacklisting).		
SR-176	E2.165		The Contractor must report all suspected or actual privacy and security violations for PWGSC e-Procurement Solution Services as Security Incidents.	IR-6	M
SR-177	E2.166		The Contractor must report all suspected or actual privacy and security violations for PWGSC e-Procurement Solution Services as Security Incidents.	IR-6	M
SR-178	E2.167	Incident Response	The Contractor must provide a Monthly Management Report (MMR) that includes: a) executive overview; b) summary of Incident activity; c) summary of security Incidents and remedial actions taken; and d) summary of patches and security patches implemented.	IR-6(2)	M
SR-179	E2.168		The Contractor must provide a monthly security threat report to PWGSC that includes: a) top 25 threat vectors; b) top 25 targeted service/protocol/applications; c) top 10 origin/source of attack; and d) top 25 types of attacks (e.g. injection, phishing, DoS, cross-site scripting, drive-by downloading, etc.).	IR-6(2)	M
SR-180	E2.169		The Contractor must provide a monthly report to Canada of all Security Incidents that includes the following information: a) Incident Ticket number; b) Incident Ticket opened/closed date; c) threat vector; d) targeted service/protocol/application; e) origin/source of attack, and f) type of attack (e.g. injection, phishing, DoS, cross-site scripting, drive-by downloading, etc.).	IR-6(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-181	E2.170		The Contractor must provide a security breach report weekly and when requested by PWGSC that includes: a) number of Security Incidents; b) number of security investigations completed; c) average/highest response time to Security Incidents, and d) average/highest security investigation completion time.	IR-6(2)	M
SR-182	E2.171		The Contractor must provide a security breach report weekly and when requested by PWGSC that includes: a) number of Security Incidents; b) number of security investigations completed; c) average/highest response time to Security Incidents, and d) average/highest security investigation completion time.	IR-6(2)	M
SR-183	E2.172		The SOC must provide the service of a Security Operations and Response Specialist who will be PWGSC's point of contact for: a) Security Incidents; b) security issues; c) requests for information on security; d) coordination of security response, and e) security alerts.	IR-6(2)	M
SR-184	E2.173		The Security Operations and Response Specialist must have the following minimum qualifications: a) have relevant experience in security operations and response; b) have in-depth knowledge of the PWGSC e-Procurement Solution; c) be capable of rapidly analyzing and assessing Incident data;	IR-6(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			d) be capable of providing a factual assessment of the situation; e) be fully trained on the PWGSC e-Procurement Solution security monitoring and reporting solution; f) be capable of rapidly responding to inquiries; g) be client oriented; h) be capable of working under high stress and pressure, and i) be bilingual.		
SR-185	E2.174	Incident Response	Meetings for Security Incidents, or security related matters as identified by PWGSC, must be in Person in the National Capital Region (NCR) during regular business hours (08:00 to 17:00 ET) Monday to Friday and during hours outside that time period as agreed to between the Contractor and PWGSC.	IR-7(2)	M
SR-186	E2.175		The Contractor must be available to participate in a Security Incident briefing provided by Canada, (e.g. for Classified briefing).	IR-7(2)	M
SR-187	E2.176	Incident Response	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance. In addition to any sources of intelligence on cyber threats and Incidents sources that The Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents	IR-8	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).		
SR-188	E2.177		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.	IR-8	M
SR-189	E2.178		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.	IR-8	M
SR-190	E2.179		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.	IR-8	M
SR-191	E2.180		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.	IR-8	M
SR-192	E2.181		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies:	IR-8	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).		
SR-193	E2.182		The Contractor must continue to automatically send e-Procurement upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-8	M
SR-195	E2.183		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.	IR-8	M
SR-196	E2.184		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.	IR-8	M
SR-197	E2.185		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible	IR-8	M
SR-198	E2.186		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service	IR-8	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.		
SR-199	E2.187		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).	IR-8	M
SR-200	E2.188		The Contractor must continue to automatically send Email upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.	IR-8	M
SR-201	E2.189		The Contractor must have proper forensic procedures and safeguards in place that includes: a) the maintenance of a chain of custody for both the audit information, and b) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.	IR-8	M
SR-202	E2.190		The Contractor must develop an incident response plan that includes: a) how The Contractor plans to identify, report, and escalate Security Incidents; b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery; c) a description of the structure and organization of the Security Incident response capability; d) a high-level approach for how the Security Incident response capability fits into The Contractor's overall organization; e) a definition of reportable Security Incidents; f) a definition of metrics for measuring the Security Incident response capability; and	IR-8	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			g) a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.		
SR-203	E2.191	System Maintenance	The Contractor must perform controlled maintenance by: a) scheduling, performing, documenting, and reviewing records of maintenance and repairs on PWGSC e-Procurement Solution Service Infrastructure components in accordance with manufacturer or vendor specifications; b) controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location; c) requiring that a designated Contractor's official explicitly approve the removal of the PWGSC e-Procurement Solution Service Infrastructure components from The Contractor data centre for off-site maintenance or repairs; d) sanitizing equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, and e) checking all potentially impacted security requirements to verify that the controls are still functioning properly following maintenance or repair actions.	MA-2, MA-2(1), MA-2(2)	M
SR-204	E2.192	System Maintenance	The Contractor must approve, control, monitor and maintain, on an ongoing basis, the hardware and software used for maintaining the PWGSC e-Procurement Solution Service Infrastructure specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).	MA-3	M
SR-205	E2.193	System Maintenance	The Contractor must a) check all media containing diagnostic and test programs for malicious code before the media are used on PWGSC e-Procurement Solution Service Infrastructure components; b) verifying that there is no PWGSC e-Procurement Solution Service information contained on the equipment;	MA-3(2), MA-3(3), MA-3(4)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) sanitizing or destroying the PWGSC e-Procurement Solution Service equipment; d) retaining the PWGSC e-Procurement Solution Service equipment within the PWGSC e-Procurement Solution Service facility or obtaining an exemption from a designated PWGSC e-Procurement Solution Service Contracting Authority explicitly authorizing removal of the equipment from the PWGSC e-Procurement Solution Service facility.		
SR-206	E2.194	System Maintenance	The Contractor must authorize, monitor, and control maintenance and diagnostic activities on the PWGSC e-Procurement Solution Service Infrastructure by: a) allowing the use of maintenance and diagnostic tools approved by PWGSC; (to be discussed) b) employing strong identification and authentication techniques in the establishment of maintenance and diagnostic sessions that tightly bound to the user and by separating the maintenance session from other network sessions with the PWGSC e-Procurement Solution Service Infrastructure by either: (i) physically separated communications paths; or (ii) logically separated communications paths using CSE-approved cryptographic modules and algorithms (see subsection Encryption Standards); c) recording maintenance and diagnostic sessions; and d) having designated personnel review the records of the maintenance and diagnostic sessions.	MA-4, MA-4(1)	M
SR-207	E2.195	System Maintenance	The Contractor must: a) sanitize equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, b) inspect and sanitize components (with regard to potentially malicious software and surreptitious implants), that have been serviced off-site before reconnecting the component to the PWGSC e-Procurement Solution Service Infrastructure; c) protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either:	MA-4(3), MA-4(4), MA-4(5), MA-4(6), MA-4(7)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			(i) Physically separated communications paths; or (ii) Logically separated communications paths based upon encryption compliant with the requirements of control SC-13. d) Maintenance personnel notify [Assignment: organization-defined personnel] when non-local maintenance is planned (i.e., date/time); e) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance; f) employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communication; and g) employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.		
SR-208	E2.196	System Maintenance	The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the e-Procurement Solution Service have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.	MA-5	M
SR-209	E2.197	Media Protection	The Contractor must provide PWGSC with the operational security procedures that includes media protection requirements specified in this SOW.	MP-1	M
SR-210	E2.198	Media Protection	The Contractor a) must restrict access to IT media (digital and non-digital) containing PWGSC e-Procurement Solution Data to authorized Operators; and b) employ mechanisms to audit access attempts and access granted.	MP-2, MP-2(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-212	E2.199	Media Protection	The Contractor must mark, in accordance with the provisions of the contract, removable IT media containing Canada information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	MP-3	M
SR-213	E2.200	Media Protection	The Contractor must: a) physically control and securely store IT media containing PWGSC e-Procurement Solution Data in accordance with the RCMP G1-001, Security Equipment Guide; and b) physically control and securely store IT media containing PWGSC e-Procurement Solution Data awaiting destruction (either on- or off-site) using PWGSC approved equipment, techniques, and procedures.	MP-4	M
SR-214	E2.201	Media Protection	The Contractor must employ cryptographic mechanisms to protect information in storage that are approved by PWGSC and are in compliance with CSE guidance (ITSG-111).	MP-4(1)	M
SR-215	E2.202	Media Protection	The Contractor must sanitize and verify IT media containing PWGSC e-Procurement Solution Data, both digital and non-digital, prior to disposal, release out of The Contractor's control, or release for reuse.	MP-6, MP-6(1)	M
SR-216	E2.203	Media Protection	The Contractor must track, control and verify media sanitization by: a) performing media sanitization in compliance with ITSG-06 (http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-eng.html) requirements for Secret information; b) recording media sanitization actions; c) testing sanitization equipment and procedure to verify correct performance at least annually; and d) sanitizing re-allocated used storage devices prior to connecting them to the PWGSC e-Procurement Service Infrastructure	MP-6(2), MP-6(3), MP-6(4), MP-6(5), MP-6(6)	M
SR-217	E2.204	Physical and Environmental Protection	The Contractor must provide PWGSC with the operational security procedures that includes physical and environmental protection requirements specified in this SOW.	PE-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-218	E2.205	Physical and Environmental Protection	The Contractor must implement role-based physical access control to its PWGSC e-Procurement Solution Service Infrastructure facilities including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access PWGSC e-Procurement Solution Service Infrastructure; g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access; h) keeping the management of The Contractor's physical access control authorizations to the PWGSC e-Procurement Solution Service Facility independent of the physical access control authorization to the facility where the PWGSC e-Procurement Solution Service Facilities are located; and i) If emergency access is required, contact the RCMP for advice.	PE-2, PE-2(1), PE-2(2), PE-2(3)	M
SR-219	E2.206	Physical and Environmental Protection	The Contractor must implement role-based physical access control to its PWGSC e-Procurement Solution Service Infrastructure facilities including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access PWGSC e-Procurement Solution Service Infrastructure; g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access; h) keeping the management of The Contractor's physical access control authorizations to the PWGSC e-	**CSE ITSG 33 Specific:** PE-2(100)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			Procurement Service Facility independent of the physical access control authorization to the facility where the PWGSC e-Procurement Service Facilities are located; and i) If emergency access is required, contact the RCMP for advice.		
SR-220	E2.207	Physical and Environmental Protection	The Contractor must provide PWGSC with a building security plan for review by PWGSC including: a) physical security layout for access control points; b) physical security zones; c) monitoring physical access points; and d) The Contractor must enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the infrastructure resides (excluding those areas within the facility officially designated as publicly accessible); i) Verify individual access authorizations before granting access to the facility; ii) Controls entry to the facility containing the infrastructure using physical access devices and/or guards; iii) Control access to areas officially designated as publicly accessible in accordance with The Contractor's assessment of risk; iv) Secure keys, combinations, and other physical access devices; v) Inventories physical access devices at least annually; and vi) Combinations and keys must be changed immediately when keys are lost, combinations are compromised, or individuals are transferred or terminated.	PE-3, PE-3(1), PE-3(2) PE-3(3), PE-3(4), PE-3(5), PE-3(6), PE-4, PE-5	M
SR-222	E2.208	Physical and Environmental Protection	The Contractor must monitor physical access to PWGSC e-Procurement Solution Service Infrastructure facilities by: a) monitoring in real-time physical intrusion alarms and surveillance equipment; b) recording all physical access events; c) reviewing physical access logs at least monthly; d) providing logs on a monthly basis and as requested by PWGSC; and e) create a Security Incident upon discovery of abnormal activity.	PE-6, PE-6(1), PE-6(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-223	E2.209	Physical and Environmental Protection	The Contractor must control physical access to PWGSC e-Procurement Solution Service Infrastructure facilities by: a) authenticating visitors before authorizing access with PWGSC approval to the facility where the infrastructure resides; b) authenticating visitors with two forms of identification prior to granting access to the PWGSC e-Procurement Solution Service facility; and c) escorting visitors and monitoring visitor activity, within the PWGSC e-Procurement Solution Facility at all times.	PE-7, PE-7(1), PE-7(2)	M
SR-224	E2.210	Physical and Environmental Protection	The Contractor must review visitor access records for the PWGSC e-Procurement Solution Facility **at least every 90 days**.	PE-8, PE-7(2)	M
SR-225	E2.211	Physical and Environmental Protection	The Contractor must protect power equipment and power cabling servicing the PWGSC e-Procurement Solution Facility from damage and destruction.	PE-9	M
SR-226	E2.212	Physical and Environmental Protection	The Contractor must implement protection devices to prevent the accidental activation of emergency power shutoff mechanisms of PWGSC e-Procurement Solution Service Infrastructure.	PE-10	M
SR-227	E2.213	Physical and Environmental Protection	The Contractor must authorize, monitor, and control all components entering and exiting the PWGSC e-Procurement Solution Service Infrastructure facilities and maintain records of those components and activities. Records must be made available monthly and as requested by GC.	PE-16	M
SR-228	E2.214	Physical and Environmental Protection	The Contractor must a) implement at alternate work sites management, operational, and technical security controls that achieve the same objectives as those implemented at the main PWGSC e-Procurement Solution Facility. b) Alternate site must be approved concurrently with the Primary sites by CISD/IISD.	PE-17, PS-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-229	E2.215	Personnel Security	The Contractor must, upon termination of an individual's employment associated with PWGSC e-Procurement Solution Services: a) terminate physical access to PWGSC e-Procurement Solution Service Infrastructure facilities for the employee; b) terminate PWGSC e-Procurement Solution Service Infrastructure access, including remote access, and c) retrieve all security-related property (e.g., employee identity card, physical authentication token).	PS-4	M
SR-230	E2.216	Personnel Security	The Contractor must manage PWGSC e-Procurement Solution Service Infrastructure privileged Operators accounts as follows: a) create Operator accounts in accordance with role-based access profiles that specify privileges; b) track and monitor Operator role assignments, and c) adjust role assignments as Operator role changes.	PS-5	M
SR-231	E2.217		The Contractor must implement role-based physical access control to its PWGSC e-Procurement Solution Service Infrastructure facilities including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access PWGSC e-Procurement Solution Service Infrastructure; g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access; h) keeping the management of The Contractor's physical access control authorizations to the Email Service Facility independent of the physical access control authorization to the facility where the Email Service Facilities are located; and i) If emergency access is required, contact the RCMP for advice.	PS-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-232	E2.218	Personnel Security	The Contractor must have access agreements to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data where: a) prior to being granted access to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data, Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) The Contractor reviews and updates access agreements to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data every two years.	PS-6	M
SR-233	E2.219	Personnel Security	The Contractor must a) prior to being granted access to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data, ensure that the Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) provide training for PWGSC e-Procurement Solution Service Infrastructure Operators in their responsibilities to protect the privacy and confidentiality of the PWGSC e-Procurement Solution Data as per the terms and conditions of the PWGSC e-Procurement Solution contract and in the sanctions for failure to comply. The Contractor must provide bi-annual refresher training.	PS-8	M
SR-234	E2.220	Risk Assessment	The Contractor must allow PWGSC, or its representatives, to conduct a Vulnerability Assessment against the PWGSC e-Procurement Solution Service, within 3 Federal Government Working Days of a request by PWGSC, that includes: a) physical access to the PWGSC e-Procurement Solution Service facilities (i.e. Contractor's facilities where the PWGSC e-Procurement Solution Service Infrastructure (i.e. hardware and software) is located); b) network access(es) to the PWGSC e-Procurement Solution Service Infrastructure to allow for authenticated and unauthenticated scanning of network components and security appliances, using PWGSC operated equipment, and PWGSC specified tools; c) assistance for the duration of any onsite portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the PWGSC e-Procurement Solution Service Infrastructure (i.e., the hardware, software, and network components, security appliances, and	RA-5	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			their configuration); (7) PWGSC will limit its Vulnerability Assessment to discovery and scanning activities to PWGSC e-Procurement Solution Service Infrastructure and will not engage in disruptive or destructive activities.		
SR-235	E2.221	Risk Assessment	The Contractor must ensure that the network access (es) to the PWGSC e-Procurement Solution Service Infrastructure to allow for authenticated and unauthenticated scanning of network components and security appliances, using PWGSC operated equipment, and PWGSC specified tools.	RA-5(5)	M
SR-236	E2.222	Risk Assessment	The Contractor must run automated vulnerability scanning tools against all PWGSC e-Procurement Solution Service Infrastructure components on a monthly basis, or as specified by PWGSC.	RA-5(7)	M
SR-237	E2.223	System and Services Acquisition	From the date vulnerabilities are formally identified, The Contractor must, at a minimum: a) Mitigate all high-risk vulnerabilities within 10 days; and b) Mitigate all moderate risk vulnerabilities within 30 days. PWGSC and Contractor will mutually agree and determine the risk rating of vulnerabilities.	SA-3	M
SR-238	E2.224		The Contractor must maintain the Email Service's security authorization state through continuous monitoring and annual audit of the implemented security requirements within the e-Procurement Service to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the e-Procurement Service and its operational environment.	SA-3	M
SR-239	E2.225		The Contractor must provide evidence to support authorization maintenance activities, within 30 days of a request by PWGSC, following all changes to the PWGSC e-Procurement Solution Service Infrastructure within The Contractor's control.	SA-3	M
SR-240	E2.226		The Contractor must update, as requested by PWGSC, and within 30 days of a request by PWGSC, security operating procedures and demonstrate implementation as part of authorization maintenance.	SA-3	M
SR-241	E2.227	System and Communications Protection	The Contractor as part of the Security Operational Procedures must include policy and procedures to facilitate the implementation and maintenance of the system and communications protection requirements specified in this SoR and in applicable GC standards specified in this SoR.	SC-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-242	E2.228	System and Communications Protection	The PWGSC e-Procurement Solution Service must include a Denial of Service (DoS) capability that limits concurrent connections as **specified by PWGSC**.	SC-5, SC-5(1), SC-5(2)	M
SR-243	E2.229	System and Communications Protection	1) The service design for PWGSC e-Procurement Solution Services must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (<insert URL link here>) and ITSG-38 (<insert URL link here>). Additionally, The PWGSC e-Procurement Solution Service Infrastructure must monitor and control communications at the external boundary of the system and at key internal boundaries within the system in compliance with ITSG-22 and ITSG-38. 2) The PWGSC e-Procurement Solution Service Contractor must monitor and analyze network traffic, in near real time, to detect attacks and evidence of compromised PWGSC e-Procurement Solution Service Infrastructure components. 3) The PWGSC e-Procurement Solution Service Contractor must detect attacks including but not limited to: a) denial of service attacks; b) malware; c) social engineering; d) unauthorized intrusion or access; e) information breach; and f) all other security breaches or cyber threats targeting Canada.	SC-7	M
SR-244	E2.230	System and Communications Protection	The PWGSC Contractor must a) physically allocate publicly accessible PWGSC e-Procurement Solution Service Infrastructure components to separate sub-networks with separate physical network interfaces; b) implement the Mobile Device Management (MDM) service in accordance with guidance in ITSG-22 and ITSG-38;	SC-7(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) implement the MDM mobile data service and connection service in its own separate physical network segment connected through a physical firewall appliance (<insert URL from CSE>) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. If this is not achievable The Contractor must obtain approval from PWGSC for alternate products; and d) implement the MDM Management Service attachment service in its own separate physical network segment connected through a physical firewall appliance (<insert URL from CSE>) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. If this is not achievable The Contractor must obtain approval from PWGSC for alternate products.		
SR-245	E2.231	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must exclusively connect to external networks or information systems specified by Canada only through managed interfaces specified by Canada using boundary protection devices arranged in compliance with ITSG-22 and ITSG-38.	SC-7(2)	M
SR-246	E2.232	System and Communications Protection	The Contractor must actively manage all network connections to external services associated with the PWGSC e-Procurement Solution Service Infrastructure as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by PWGSC; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.	SC-7(4), SC-7(5)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-247	E2.233	System and Communications Protection	The Contractor must prevent Contractor managed devices (e.g.: notebook or other device used for administration) that are connected with the PWGSC e-Procurement Solution Service Infrastructure from communicating outside of that communications path (e.g. accessing the Internet via a separate connection available to the device).	SC-7(7)	M
SR-248	E2.234	System and Communications Protection	1) The PWGSC e-Procurement Solution Service Infrastructure must route internal network traffic to external networks through authenticated proxy servers as defined by PWGSC within the managed interfaces of boundary protection devices. 2) The PWGSC e-Procurement Solution Service Design must allow Mobile Device traffic to pass through a Canada Internet proxy **as specified by PWGSC**.	SC-7(8)	M
SR-249	E2.235	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must detect extrusion events in **near real time**.	SC-7(9)	M
SR-250	E2.236	System and Communications Protection	The Contractor must monitor and analyze hosts behaviours (Host-based Intrusion Detection and Prevention) in near real-time to detect attacks and evidence of compromised hosts	SC-7(12)	M
SR-251	E2.237	System and Communications Protection	The Contractor must a) physically separate the network IP traffic of the PWGSC e-Procurement Solution System Data from the PWGSC e-Procurement Solution Service Management Data and PWGSC e-Procurement Solution Service User Data. b) Logically separate the network IP traffic between the PWGSC e-Procurement Solution Service Management Data and the PWGSC e-Procurement Solution User Data.	SC-7(13)	M
SR-252	E2.238	System and Communications Protection	The Contractor must configure boundary protections (i.e. firewall) to fail safe (i.e. no traffic goes through) upon failure.	SC-7(18)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-253	E2.239	System and Communications Protection	The PWGSC e-Procurement Solution Service Design a) must allow mutual authentication of connections, between the e-Procurement Solution Service and other domains as specified by PWGSC, and exclusively exchange information with these other domains using mutual authentication. b) Must ensure that the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC.	SC-8	M
SR-254	E2.240	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure a) must protect the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards). unless otherwise protected by alternative physical measures approved by PWGSC; and b) must protect the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards) unless otherwise protected by alternative physical measures approved by PWGSC.	SC-8(1)	M
SR-255	E2.241	System and Communications Protection	The PWGSC e-Procurement Solution Service Design must a) allow mutual authentication of connections, between the e-Procurement Service and other domains as specified by PWGSC, and exclusively exchange e-Procurement Messages with these other domains using mutual authentication; b) ensure that the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC; c) conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (<insert URL here>) and ITSG-38 (<insert URL here>); and	SC-9, SC-9(1), Sc-9(2), SC-12(1), SC-12(2), SC-12(3), SC-12(4), SC-12(5), **CSE ITSG-33 Specific:** SC-9(100)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			d) encrypt Security Incident information with approved cryptographic standards (see subsection Encryption Standards) if the information is sent in electronic form.		
SR-256	E2.242	System and Communications Protection	The Contractor must actively manage all network connections to external services associated with the PWGSC e-Procurement Solution Service Infrastructure as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by PWGSC; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.	SC-10	M
SR-258	E2.243	System and Communications Protection	The PWGSC e-Procurement Solution Service Design must ensure that a) cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for PWGSC e-Procurement Solution Services: i) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSA-11E (http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-eng.html) or in a subsequent version; ii) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-eng.html) to at least FIPS 140-2 validation at Level 1, and iii) operate in FIPS Mode. b) the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at	SC-13, **CSE ITSG-33 Specific:** SC-13(100), SC-13(101)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC.		
SR-260	E2.244	System and Communications Protection	The PWGSC e-Procurement Solution Service Design must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-eng.pdf) and ITSG-38 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-eng.pdf).	SC-14	M
SR-261	E2.245	System and Communications Protection	The Contractor must not prohibit a User to encrypt, decrypt, sign and verify PWGSC e-Procurement Solution attachment files using Certificates trusted by the GC-CA.	SC-17	M
SR-262	E2.246	System and Communications Protection	The Contractor must only allow pre-approved mobile code in the PWGSC e-Procurement Solution Service Infrastructure thus denying any other mobile code from being downloaded and executed.	SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4)	M
SR-263	E2.247	System and Communications Protection	The Contractor must prohibit the use of VoIP technologies in the PWGSC e-Procurement Solution Service Infrastructure unless specifically authorized by PWGSC.	SC-19	M
SR-264	E2.248	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure component or components that collectively provide name/address resolution service for the PWGSC e-Procurement Solution Service must implement internal/external role separation.	SC-22	M
SR-265	E2.249	System and Communications Protection	The PWGSC e-Procurement Solution Service must allow authentication of the following Software Client types with an X.509 credential using mutual transport layer authentication (TLS): a) Web Browser Clients; and b) Mobile Browser Clients.	SC-23	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-266	E2.250		The PWGSC e-Procurement Solution Service must allow the authentication of all types of Software Clients with a PWGSC e-Procurement Solution Service credential.	SC-23	M
SR-267	E2.251	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must invalidate session identifiers upon operator logout or other session termination.	SC-23(1)	M
SR-268	E2.252	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must use a readily observable logout capability whenever authentication is used to gain access to PWGSC e-Procurement Solution Service Infrastructure components.	SC-23(2)	M
SR-269	E2.253	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must a) generate a unique session identifier for each session with randomness using CSE-approved cryptography (see subsection Cryptographic Standards); and b) recognize only session identifiers that are generated by the PWGSC e-Procurement Solution Service Infrastructure.	SC-23(3), SC-23(4)	M
SR-270	E2.254	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must protect the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards) unless otherwise protected by alternative physical measures approved by PWGSC.	SC-28	M
SR-271	E2.255	System and Communications Protection	The Contractor must a) create one or more Incident Tickets for each Incident detected by The Contractor or reported by PWGSC; and b) physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in PWGSC dedicated storage.	SC-28(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-272	E2.256	System and Communications Protection	Where layered safeguards are implemented (defence-in-depth solutions), the Contractor must implement solutions from different vendors at different layers within the network.	SC-29	M
SR-273	E2.257	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must be physically and/or using virtualization technology, dedicated to PWGSC. The Contractor, at their discretion, can use non-dedicated hardware, non-dedicated software for the operation, administration and management of PWGSC e-Procurement Solution Service Management Data. Any use of non-dedicated hardware, non-dedicated software is only allowed for Email Solution Service Management Data according to the following conditions: a) must not access, process or store PWGSC e-Procurement Solution User Data; b) must not access, process or store PWGSC e-Procurement Solution System Data; c) must not access, process or store user account names and passwords; d) must be logically segregated from other client's data; e) must adhere to all PWGSC e-Procurement Solution Service Infrastructure requirements outlined in Annex 2 Security Requirements; f) must not access, process or store information labeled as Protected or Classified unless approved in writing by PWGSC; g) must not access, process or store service design information for the PWGSC e-Procurement Solution Service; and h) must not allow for the control or modification of the PWGSC dedicated PWGSC e-Procurement Solution Service Infrastructure.	SC-32	M
SR-274	E2.258		The PWGSC e-Procurement Solution Service must include dedicated controls for any network interconnections between dedicated and non-dedicated PWGSC e-Procurement Solution Service Infrastructure, according to the approved Security Design, that includes: a) boundary protection whereby, the Contractor must use current or previously evaluated physical firewall appliances (http://www.cse-cst.gc.ca/its-sti/services/cc/index-eng.html) validated under a	SC-32	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. The Contractor must obtain approval from PWGSC for alternative physical firewall appliances; b) integration of PWGSC provided threat detection equipment; c) incorporation of Contractor provided threat detection/prevention solutions; d) routing of traffic through authenticated proxy servers; and e) role based access control with least privilege.		
SR-275	E2.259		The Contractor must a) physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in PWGSC dedicated storage; b) ensure that any network configuration details contained in any asset records and configuration records management systems for the PWGSC e-Procurement Solution Service Infrastructure are encrypted.; c) physically separate the network IP traffic of the PWGSC e-Procurement Solution System Data from all other PWGSC e-Procurement Solution Data; and d) logically separate the network IP traffic between the PWGSC e-Procurement Solution Service Management Data and the PWGSC e-Procurement Solution User Data.	SC-32	M
SR-276	E2.260		The categorization of data for PWGSC e-Procurement Solution Services as either PWGSC e-Procurement Solution System Data, PWGSC e-Procurement Solution User Data or PWGSC e-Procurement Solution Service Management Data will be at the sole discretion of PWGSC and based on comparison to other similar data.	SC-32	M
SR-277	E2.261	System and Information Integrity	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that includes operational roles and responsibilities for system and information integrity requirements specified in this SOW.	SI-1	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-278	E2.262	System and Information Integrity	The Contractor must define and execute the processes for patch management for the PWGSC e-Procurement Solution Infrastructure components that includes: a) ensuring the latest version of applications and operating systems are used; b) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; c) prioritizing critical patches using a risk-based approach; d) taking applications offline and bringing them back online; e) aligning criticality levels for patches as specified by PWGSC; f) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; and g) testing and verification methodology to ensure that patches have been implemented properly. h) defines the processes for patch management on custom software utilized within the PWGSC e-Procurement Solution Service Infrastructure that includes: i) identifying, reporting, and correcting flaws in custom software; ii) testing software updates related to flaw remediation for effectiveness and potential side effects on the Email Service before installation; iii) incorporating flaw remediation into the Email Service configuration management process;	SI-2, SI-2(1), SI-2(2), SI-2(3), SI-2(4)	M
SR-279	E2.263	System and Information Integrity	The Contractor must a) centrally manage the malicious code protection mechanisms; b) automatically updates malicious code protection/malware mechanisms (including signature definitions) within 6 hours of availability and as requested by PWGSC; c) prevents non-privileged users from circumventing malicious code protection capabilities; d) updates malicious code protection mechanisms only when directed by a privileged user; and e) does not allow users to introduce removable media into the PWGSC e-Procurement Solution Service Infrastructure.	SI-3(1), SI-3(2), SI-3(3), SI-3(4), SI-3(5)	M
SR-280	E2.264	System and Information Integrity	The Contractor must actively manage all network connections to external services associated with the PWGSC e-Procurement Solution Service Infrastructure as follows: a) deny all network traffic by default;	SI-4(4), SI-4(11)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by PWGSC; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and, and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies).		
SR-281	E2.265	System and Information Integrity	The PWGSC e-Procurement Solution Service Infrastructure must provide near real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.	SI-4(5)	M
SR-282	E2.266	System and Information Integrity	The PWGSC e-Procurement Solution Service Infrastructure must prevent all non-privileged users from circumventing intrusion detection and prevention capabilities.	SI-4(6)	M
SR-283	E2.267	System and Information Integrity	The PWGSC e-Procurement Solution Service Infrastructure **Security Event and Log Management Solution** must: a) include centralized and time-synchronised logging of allowed and blocked PWGSC e-Procurement Solution activity with regular log analysis; b) keep 3 months of events and logs online; c) keep events and logs associated with a security Incident for at least 2 years; d) store logs for at least 1 year; e) categorize events and logs based on Partners; and f) protect data and audit logs from unauthorized access, modification, and deletion.	SI-4(8)	M
SR-284	E2.268	System and Information Integrity	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives;	SI-5, SI-5(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance. In addition to any sources of intelligence on cyber threats and Incidents sources that the Contractor monitors in its routine operations, the Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).		
SR-285	E2.269	System and Information Integrity	The Contractor must implement a centrally managed Integrity Verification Solution to detect unauthorized changes to software and Email Infrastructure component configuration including: a) performing integrity scans at least every 30 days, and b) automatically generating a Security Incident Ticket upon discovering discrepancies during integrity verification.	SI-7, SI-7(1), SI-7(2)	M
SR-286	E2.270	System and Information Integrity	The PWGSC e-Procurement Solution Service Anti-Virus/Anti-Spam (AVS) Service must a) scan outbound and inbound messages for spam content in real-time; b) identify a message as spam based on a spam probability score (high, medium, low) specified by PWGSC; c) assign each spam classification as specified by PWGSC and an action to be taken if that threshold is exceeded; d) The Email AVS Service must respond to an Email Message identified as spam, as specified by PWGSC, that includes: a) discarding the Email Message (e.g. confirmed spam); b) tagging the subject field of the Email Message;	SI-8, SI-8(1)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c) sending the Email Message to a Mailbox and Email Folder specified by PWGSC (e.g. junk mail); d) replying to the Email Message with a bilingual warning message in the subject field, message body, and message header; and e) allowing the Email Message to be delivered based on content criteria specified by PWGSC (for example, words found in an Email subject line). c) Reject the message; d) Redirect the message; e) Quarantine the message; f) Modify the subject header of the message; g) support configuration of i) SPAM blacklists to allow customized entries as specified by PWGSC; ii) SPAM whitelists to allow customized entries as specified by PWGSC; and iii) the sensitivity of the heuristic analysis as specified by PWGSC. h) make use of a Sender IP Reputation Service that shall accept or reject SMTP connections based on the reputation of the sender IP address, before the message is accepted for processing; i) The Sender IP Reputation Service shall include in its reputation verification hosts that are published in a public DNS Block List (DNSBL); j) If the reputation score for a sender IP address exceeds a configurable threshold, the Sender IP Reputation Service shall reject the sender's SMTP connections; and k) System events related to Sender IP reputation service will be logged and sent to Canada.		
SR-287	E2.271	System and Information Integrity	The PWGSC e-Procurement Solution AVS Service must a) automatically update spam signature updates automatically at regular intervals to ensure that the SPAM signatures are always up to date and based on analysis of SPAM messages collected from various external SPAM databases by the Contractor; b) automatically update spam signatures and Spam Blacklists within 15 minutes of availability or at frequency specified by PWGSC; and c) apply security updates of signatures and Spam Blacklists within 15 minutes of receiving the updates.	SI-8(2)	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-288	E2.272	System and Information Integrity	The PWGSC e-Procurement Solution Service, where assisted data entry is required in the input fields with pre-defined values are populated using lists, drop-down lists, checkboxes and radio buttons in plain language; a) assisted data entry where input fields with embedded meaning (i.e. multiple data elements concatenated within the same input field) are populated using a combination of lists, drop-down lists, checkboxes and radio buttons in plain language for predefined values and textboxes for user provided values; b) error verification where input fields are verified for format and validity, including cross-field validation, with detailed error messages in plain language that indicate to the user what is incorrect and what is the rule(s) that failed; and c) pre-defined fields (e.g. service, work type, contact name, unit pricing, item number, quantities, etc.) approved by PWGSC, with assisted data entry (where applicable) to minimize error entries.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-289	E2.273	Data Security & Information Lifecycle Management Data Inventory / Flows	The PWGSC e-Procurement Solution Service policies and procedures must be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, Contractor must ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-291	E2.274	Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	The PWGSC e-Procurement Solution Service policies and procedures must be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance must be implemented for objects that act as aggregate containers for data.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-292	E2.275	Data Security & Information Lifecycle Management Non-Production Data	The PWGSC e-Procurement Solution Service production data must not be replicated or used in non-production environments.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-293	E2.276	Data Security & Information Lifecycle Management Ownership / Stewardship	All PWGSC e-Procurement Solution Service data must be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-294	E2.277	Data Security & Information Lifecycle Management Secure Disposal	Any use of PWGSC e-Procurement Solution Service Production data in non-production environments requires explicit, documented approval from PWGSC whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-295	E2.278	Datacenter Security Asset Management	The PWGSC e-Procurement Solution Service assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time must be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-296	E2.279	Datacenter Security Controlled Access Points	The PWGSC e-Procurement Solution Service physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) must be implemented to safeguard sensitive data and information systems.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-297	E2.280	Datacenter Security Equipment Identification	The Contractor must ensure that automated equipment identification is used as a method of connection authentication for PWGSC e-Procurement Solution Service infrastructure as approved by the PWGSC to validate connection authentication integrity based on known equipment.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-298	E2.281	Datacenter Security Off-Site Authorization	PWGSC authorization must be obtained prior to relocation or transfer of the PWGSC e-Procurement Solution Service hardware, software, or data to an offsite premises.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-299	E2.282	Datacenter Security Off-Site Equipment	The PWGSC e-Procurement Solution Service operational policies and procedures must be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This must include a wiping solution or destruction process that renders recovery of information impossible. The erasure must consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-300	E2.283	Datacenter Security Policy	The PWGSC e-Procurement Solution Service operational policies and procedures must be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-301	E2.284	Datacenter Security - Secure Area Authorization	The PWGSC e-Procurement Solution Service specific ingress and egress to secure areas must be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-302	E2.285	Datacenter Security Unauthorized Persons Entry	The PWGSC e-Procurement Solution Service specific ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises must be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-303	E2.286	Datacenter Security User Access	All physical access to the PWGSC e-Procurement Solution Service information assets and functions by users and support personnel must be restricted.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-304	E2.287	Encryption & Key Management Entitlement	The PWGSC e-Procurement Solution Service PKI keys must have identifiable owners (binding keys to identities) and there must be key management policies.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-305	E2.288	Encryption & Key Management Key Generation	The PWGSC e-Procurement Solution Service operational policies and procedures must be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, Contractor must inform the PWGSC of changes within the cryptosystem, especially if the PWGSC e-Procurement Solution Service data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-306	E2.289	Encryption & Key Management Sensitive Data Protection	The PWGSC e-Procurement Solution Service operational policies and procedures must be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-306	E2.290	Encryption & Key Management Storage and Access	The PWGSC e-Procurement Solution Service platform and data-appropriate encryption (in compliance with CSE guidance ITSG-111) in open/validated formats and standard algorithms must be required. Keys must not be stored in the cloud (i.e. at the e-Procurement Solution Service cloud Contractor in question), but maintained by the PWGSC or trusted key management Contractor as mutually agreed upon with PWGSC. The PWGSC e-Procurement Solution Service key management and key usage must be separated duties.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-307	E2.291	Governance and Risk Management Data Focus Risk Assessments	The PWGSC e-Procurement Solution Service risk assessments associated with data governance requirements must be conducted at planned intervals as mutually agreed upon with PWGSC and must consider the following: a) Awareness of where sensitive data is stored and transmitted across applications, databases, servers,	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			and network infrastructure; b) Compliance with defined retention periods and end-of-life disposal requirements; and c) Data classification and protection from unauthorized use, access, loss, destruction, and falsification.		
SR-308	E2.292	Governance and Risk Management Management Oversight	The PWGSC e-Procurement Solution Service managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-309	E2.293	Governance and Risk Management Management Program	The PWGSC Contractor must have an Information Security Management Program (ISMP) developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program must include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: a) Risk management b) Security policy c) Organization of information security d) Asset management e) Human resources security f) Physical and environmental security g) Communications and operations management h) Access control i) Information systems acquisition, development, and maintenance	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-309	E2.294	Governance and Risk Management Management Support/Involvement	The PWGSC Contractor executive and line management must take formal action to support information security through clearly-documented direction and commitment, and must ensure the action has been assigned.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-310	E2.295	Governance and Risk Management Policy	The PWGSC Contractor information security policies and procedures must be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-311	E2.296	Governance and Risk Management Policy Impact on Risk Assessments	The PWGSC e-Procurement Solution Service risk assessment results must include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-312	E2.297	Governance and Risk Management Policy Reviews	The PWGSC Contractor's business leadership (or other accountable business role or function) must review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-313	E2.298	Governance and Risk Management Risk Management Framework	All PWGSC e-Procurement Solution Service risks must be mitigated to an acceptable level. Acceptance levels based on risk criteria must be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-314	E2.299	Human Resources Asset Returns	The Contractor upon termination of workforce personnel and/or expiration of external business relationships, all PWGSC e-Procurement Solution Service-owned assets must be returned within an established period.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-315	E2.300	Human Resources Employment Termination	The Contractor roles and responsibilities for performing employment termination or change in employment procedures for PWGSC e-Procurement Solution Service must be assigned, documented, and communicated.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-316	E2.301	Human Resources Mobile Device Management	The Contractor must establish policies, procedures, supporting business processes, and implement technical measures, to manage business risks associated with permitting mobile device access to PWGSC e-Procurement Solution Service resources and must enforce the implementation of higher	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring) as approved by PWGSC.		
SR-317	E2.302	Human Resources Roles / Responsibilities	The Contractor must document the roles and responsibilities of contractors, employees, and third-party users as they relate to PWGSC e-Procurement Solution Service information assets and security.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-318	E2.303	Human Resources Technology Acceptable Use	Policies and procedures must be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of Contractor-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to Contractor's corporate resources (i.e., BYOD) must be considered and incorporated as appropriate.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-320	E2.304	Human Resources User Responsibility	All Contractor personnel must be made aware of their roles and responsibilities for: a) Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations; and b) Maintaining a safe and secure working environment	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-321	E2.305	Human Resources Workspace	Policies and procedures must be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-322	E2.306	Infrastructure & Virtualization Security Clock Synchronization	The PWGSC Contractor must use a reliable and mutually agreed upon external time source to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-323	E2.307	Security Incident Management, E-Discovery & Cloud	The PWGSC e-Procurement Solution Service must establish policies, procedures, and supporting business processes and technical measures implemented, to triage security-related events and ensure	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
		Forensics Incident Management	timely and thorough incident management, as per established IT service management policies and procedures approved by PWGSC.		
SR-324	E2.308	Security Incident Management, E-Discovery & Cloud Forensics Incident Reporting	The PWGSC Contractor workforce personnel and external business relationships must be informed of their responsibilities and, if required, must consent and/or contractually agree to report all information security events in a timely manner. Information security events must be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-325	E2.309	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Legal Preparation	The PWGSC Contractor must implement proper forensic procedures, including chain of custody, as required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, PWGSC and/or other external business partners impacted by a security breach must be given the opportunity to participate as is legally permissible in the forensic investigation.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-326	E2.310	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Metrics	The PWGSC Contractor must put in place mechanisms to monitor and quantify the types, volumes, and costs of information security incidents.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-327	E2.311	Supply Chain Management, Transparency and Accountability	The PWGSC Contractor must a) inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks; and b) design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
		Data Quality and Integrity			
SR-328	E2.312	Supply Chain Management, Transparency and Accountability Incident Reporting	The PWGSC Contractor must make security incident information available to all affected customers, including PWGSC and Contractors periodically through electronic methods (e.g. portals).	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-329	E2.313	Supply Chain Management, Transparency and Accountability Contractor Internal Assessments	The PWGSC Contractor must perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-330	E2.314	Supply Chain Management, Transparency and Accountability Supply Chain Agreements	The PWGSC Contractor must incorporate at least the following mutually-agreed upon provisions and/or terms: a)Scope of business relationship and services offered (e.g., PWGSC (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of PWGSC Contractor and PWGSC (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) b) Information security requirements, PWGSC Contractor and PWGSC (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			c)Notification and/or pre-authorization of any changes controlled by the PWGSC Contractor with PWGSC (tenant) impacts d) Timely notification of a security incident (or confirmed breach) to all PWGSC (tenant) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) e) Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed f) Expiration of the business relationship and treatment of PWGSC (tenant) data impacted g) PWGSC (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence		
SR-331	E2.315	Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	The PWGSC Contractor must review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-332	E2.316	Supply Chain Management, Transparency and Accountability Supply Chain Metrics	The PWGSC Contractor must a) implement Policies and procedures to ensure the consistent review of service agreements (e.g., SLAs) between contractor and PWGSC (tenant) across the relevant supply chain (upstream/downstream). b) Perform at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-333	E2.317	Use of Zone Interface Point Firewall	The PWGSC e-Procurement Solution Service Design Boundary system in all Zone Interface Point (ZIP) must contain firewalls which perform state full packet inspection for infrastructure containing applications of **MEDIUM injury** and / or higher	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
			PWGSC Selections: - All PAZs, RZs, HRZs, SAZs, REZs - All zones of high and very high injury		
SR-334	E2.318	Use of Zone Interface Point Firewall	The Contractor must ensure that all firewalls in all Zone Interface Point (ZIP) must be at minimum EAL4 certified (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-335	E2.319	Use of Internal Boundary System Firewall	The Contractor must use firewalls which perform stateful packet inspection in internal boundary systems within all zone(s) for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-336	E2.320	Use of Internal Boundary System Firewall	The Contractor must use physical firewall in internal boundary systems within a all zone(s) for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-337	E2.321	Use of Internal Boundary System Firewall	The PWGSC e-Procurement Solution Service Infrastructure firewalls in all internal boundary systems must be at minimum EAL4 or common criteria certified (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-338	E2.322	Use of Internal Boundary System Physical Devices	The PWGSC e-Procurement Solution Service Internal boundary systems in all zone(s) must contain physical or virtual devices for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-339	E2.323	Zone Internetwork Device Partitioning	The PWGSC e-Procurement Solution Service infrastructure use of virtual devices in the zone internetwork must be sufficiently partitioned from virtual servers in all zones for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-340	E2.324	Use of Zone Internetworking Physical Devices	The Contractor must use physical and/or virtual devices as approved by PWGSC in the zone internetwork in all zones for infrastructure containing applications of PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-341	E2.325	Internetworking Traffic Partitioning	The PWGSC e-Procurement Solution Service Design specific virtual devices in the zone internetwork must not perform routing in Management and Restricted zones for infrastructure containing e-Procurement databases.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-342	E2.326	Storage Partitioning	PWGSC e-Procurement Solution Storage used by the hypervisor for virtual device images must be **physically and/or logically** partitioned for PWGSC e-Procurement Solution infrastructure containing applications of PROTECTED B with MEDIUM injury as defined by PWGSC.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-343	E2.327	Use of Hypervisor Features	The PWGSC e-Procurement Solution Service Design specific Virtual machines must not use any machine to machine sharing mechanism (e.g. file sharing) which is implemented within the hypervisor	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-344	E2.328	Virtual Machine Distribution	The PWGSC e-Procurement Solution Service specific Virtual machines must be distributed via a **random, pseudo random or other** algorithm as approved by PWGSC.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-345	E2.329	Virtual Machine Distribution	The PWGSC e-Procurement Solution Service Design specific Virtual machines must be distributed such that there are **at least five machines sharing** any physical resource for all physical resources.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-346	E2.330	Hypervisor Certification	The Contractor must use current or previously evaluated hypervisors managing all zones, as defined within the CSE ITSG-22 (https://cse-cst.gc.ca/en/node/268/html/15236) & ITSG-38 (https://cse-cst.gc.ca/en/node/266/html/25034) guidelines, (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers hypervisor evaluation for virtual machines protection between zones or obtain approval from PWGSC for alternative products	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-347	E2.331	ICAM	The Contractor's Interim ICAM Solution must remove all credentials once fully migrated to Canada's GC ICAM solution.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-348	E2.332	Datacenter Security	The PWGSC e-Procurement Solution Service equipment and infrastructure must be housed by the Contractor in a suitable facility that is rated as Tier "II" Data Center at minimum by Uptime Institute "Tier Standard: Operational Sustainability" (https://uptimeinstitute.com/consulting-certification/operations/tier-certification-of-operational-sustainability) or equivalent, equipped with but not limited to the following features. a) Redundant high speed internet connectivity through multiple carriers; b) Redundant computer grade HVAC; c) Redundant UPS and Generators; d) Multi-homed internet backbone; e) 24/7 monitoring and server support; f) Firewall security and Intrusion detection; and g) Physical security measures to prohibit access by unauthorized parties.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-349	E2.333	Infrastructure & Virtualization Security Change Detection	The Contractor must ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-350	E2.334	Infrastructure & Virtualization Security Management - Vulnerability Management	The Contractor must ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware) within the PWGSC e-Procurement Solution Service.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-351	E2.335	Infrastructure & Virtualization Security Network Security	The Contractor must ensure that the network environments and virtual instances must be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations must be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls as approved by PWGSC.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-352	E2.336	Infrastructure & Virtualization Security OS Hardening and Base Conrols	The Contractor must ensure that each operating system used within the PWGSC e-Procurement Solution Service is hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-353	E2.337	Infrastructure & Virtualization Security Production / Non-Production Environments	The PWGSC e-Procurement Solution Service production and non-production environments must be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties as approved by PWGSC.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-354	E2.338	Infrastructure & Virtualization Security Segmentation	The Contractor's multi-tenant e-Procurement Solution Service-owned or managed (physical and virtual) applications, and infrastructure system and network components, must be designed, developed, deployed and configured such that provider and PWGSC (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: a) Established policies and procedures; b) Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance; and c) Compliance with legal, statutory and regulatory compliance obligations.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-355	E2.339	Infrastructure & Virtualization Security VM Security - vMotion Data Protection	The Contractor must use secured and encrypted communication channels when migrating physical servers, applications, or data to virtualized servers associated with PWGSC e-Procurement Solution Service and, where possible, must use a network segregated from production-level networks for such migrations.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-356	E2.340	Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	The Contractor must ensure that access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems for PWSGC e-Procurement Solution Service be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-357	E2.341	Infrastructure & Virtualization Security Wireless Security	The Contractor PWGSC e-Procurement Solution Service policies and procedures must be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: a) Perimeter firewalls implemented and configured to restrict unauthorized traffic b) Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings); c) User access to wireless network devices restricted to authorized personnel; and d) The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network.	Tailored based on Industry Best Practices and Departmental Guidance	M

Table 4: EPS Security Requirements

Security Requirement IDs for Canada's purpose only	EPS RFP ID	Requirement Category	Description	FedRAMP Security Control ID (NIST 800-53)Reference Mapping (for Information purpose ONLY)	Type (M – Mandatory, R – Rated, F – Future)
SR-358	E2.342	Infrastructure & Virtualization Security Network Architecture	The PWGSC e-Procurement Solution Service network architecture diagrams must clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures must be implemented as approved by PWGSC and must apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Tailored based on Industry Best Practices and Departmental Guidance	M
SR-359	E2.343	Interoperability & Portability Virtualization	The Contractor must use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and must have documented custom changes made to any hypervisor in use and all PWGSC e-Procurement solution-specific virtualization hooks available for PWGSC review.	Tailored based on Industry Best Practices and Departmental Guidance	M

Section II – Security Requirements Traceability Matrix

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.1	Access Control	The Contractor must a) develop, disseminate, and review/update annually, the access control policies and associated access control requirements for e-Procurement Solution Service Infrastructure components; and b) provide PWGSC with the operational security procedures that include operational roles and responsibilities for access control.						
E2.2	Access Control	The Identity Credential and Access Management Service must automatically provision Accounts for PWGSC e-Procurement Solution Service User Accounts and Generic Accounts, as follows: a) assign a unique e-Procurement Solution Service Account and Display Name in accordance with the standard defined in subsection , by applying configurable naming and conflict resolution rules; b) create an Account with no privileges; c) assign a one-time temporary password to the Account; d) assign Account attributes and security access privileges **as specified by PWGSC**; and e) return the assigned e-Procurement Solution Service Account, Display Name, **Partner Unique Key, Supplier Unique Key** and one-time password to the Account Requester.						
E2.3		The Identity Credential and Access Management Service must a) prevent the re-use of an e-Procurement Solution Service Account as specified by PWGSC; b) allow Account suspension policies as specified by PWGSC; c) not allow access to a suspended Account; d) not allow an Account to send and receive e-Procurement Solution Service work flow messages if the Account is suspended;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		and e) not allow direct access to the PWGSC e-Procurement Solution Service Solution Service Infrastructure for any Account, as specified by PWGSC.						
E2.4	Access Control	The Contractor must manage PWGSC e-Procurement Solution Service Infrastructure Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the PWGSC e-Procurement Solution Service Infrastructure and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) notifying account administrator when temporary accounts are no longer required and when PWGSC e-Procurement Solution Service Infrastructure Operators are terminated, transferred, or PWGSC e-Procurement Solution Service Infrastructure usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year; k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators; iii) accounts after a number of day of inactivity as specified by						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		PWGSC, and iv) temporary and emergency accounts over a given age; l) granting access to the e-Procurement Service Infrastructure based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by The Contractor or PWGSC; m) reviewing accounts at least monthly; n) locking the account **after 10 unsuccessful login attempts** occurring **within five (5) minutes**, and o) keeping the account locked until manually unlocked by another Operator.						
E2.5	Access Control	The PWGSC e-Procurement Solution Service must log the following events: a) Account creation; b) Account modifications c) Account suspension; d) Account termination; e) Account deletion; and f) Account views of e-Procurement Solution Service accounts of which the User is not the primary owner.						
E2.6	Access Control	The Contractor must a) define a working hours policy and monitor PWGSC e-Procurement Solution Service Infrastructure Operators accounts utilization against that policy including: i) logging atypical usage of Operator accounts; and ii) alerting designated resources of atypical usage of Operator accounts. b) provide the PWGSC e-Procurement Solution Service Infrastructure Operators accounts atypical utilization log to						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		PWGSC within **one (1) Business Day** of a request by PWGSC; and c) ensure that PWGSC e-Procurement Solution Service Infrastructure Operators log out at the end of their working shift.						
E2.7	Access Control	The PWGSC e-Procurement Solution Service Infrastructure must enforce access authorizations for Operators.						
E2.8	Access Control	The PWGSC e-Procurement Solution Service's Data Loss Prevention (DLP) capability must a) detect violations of data loss prevention policies and apply response actions, as specified by PWGSC, that include: i) blocking transfer of the transaction; ii) blocking transfer of the transaction and return a transaction to the Sender; and iii) other actions agreed to between The Contractor and PWGSC; b) allow real-time enforcement of data loss prevention policies based on the contents of any of the following PWGSC e-Procurement Solution transaction attributes: i) strings, string patterns, and keywords within the transaction body; ii) file type of any attachments; iii) Sender domain; iv) Recipient domain; v) Sender; and vi) Recipient.						
E2.9	Access Control	The PWGSC e-Procurement Solution Service must open and scan unencrypted transactions in order to enforce policy against the contents of popular file types as specified by PWGSC.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.10	Access Control	The Contractor must implement separation of duties for Operators, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the Operator.						
E2.11	Access Control	The Contractor must implement a least privileges policy for PWGSC e-Procurement Solution Service Infrastructure Operators as follows: a) the access control mechanisms must be configured to implement least privilege, allowing only authorized accesses for Operators (and processes acting on their behalf) that are necessary to accomplish assigned tasks; b) create non-privileged accounts to be used for non-operations tasks; c) restrict authorization to super user accounts (e.g., root) to designated Operators; d) restrict sharing of Operator accounts; and e) must uniquely identify the human Operator who has performed each operation on the PWGSC e-Procurement Solution Service Infrastructure.						
E2.12	Access Control	The PWGSC e-Procurement Solution Service must automatically lock an Account following a number of unsuccessful login attempts as specified by PWGSC.						
E2.13	Access Control	The PWGSC e-Procurement Solution Service must display a logon banner approved by PWGSC on the login page of any web-based application for Users.						
E2.14		The PWGSC e-Procurement Solution Service Infrastructure must include an access control mechanism that:						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		a) prevents access to PWGSC e-Procurement Solution Service Infrastructure components or resources without identification, authentication, and authorization; b) displays a PWGSC-approved logon warning banner that authorized operators must acknowledge prior to being granted access to PWGSC e-Procurement Solution Service Infrastructure components; c) notifies the operators, upon successful logon (access), of the date and time of the last logon (access), and d) uses a readily observable logout capability whenever authentication is used to gain access to PWGSC e-Procurement Solution Service Infrastructure components.						
E2.15		The PWGSC e-Procurement Solution Service Infrastructure access control mechanisms must include an operator session lock mechanism that: a) prevents further access to Infrastructure components by automatically initiating an operator session lock after a period of inactivity **no longer than 60 minutes**; b) prevents further access to Infrastructure components by initiating an operator session lock when requested by the operators; c) displays a screen saver that contains no meaningful information to completely replace what was previously displayed on the screen upon activation of an operator session lock, and d) unlocks an operator session after successful authentication of the operator.						
E2.16	Access Control	The Contractor must ensure that any use of Remote Management within the PWGSC e-Procurement Solution Service Infrastructure take place using a method approved by PWGSC that includes: a)Remote Management must be restricted to PWGSC e-						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		Procurement Solution Service Infrastructure located within a contractor Service Delivery Point using PWGSC e-Procurement Solution dedicated management consoles; b)Documenting allowed methods of Remote Management and establish usage restrictions and implementation guidance for each allowed remote management method; c) monitoring for unauthorized Remote Management; d) authorizing Remote Management prior to connection; e) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods; f) routing all Remote Management to PWGSC e-Procurement Solution Service Infrastructure components through a limited number of managed access control points; g) protecting information about Remote Management mechanisms from unauthorized use and disclosure; and h) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods.						
E2.17	Access Control	The Contractor must not allow wireless access to the PWGSC e-Procurement Solution Service Infrastructure from within the data center facility for privileged users including operators.						
E2.18	Access Control	The Contractor must: a) continuously monitor for wireless access points on the PWGSC e-Procurement Solution Service Infrastructure within the Data Center Facility; b) immediately disable any wireless access point when one is discovered, and c) open a security Incident Ticket if a wireless access point is discovered.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.19	Access Control	The Contractor must permanently disable all wireless networking functions internally embedded within PWGSC e-Procurement Solution Service Infrastructure.						
E2.20	Access Control	The Contractor must not allow a) Mobile Devices to access the PWGSC e-Procurement Solution Service Infrastructure from within the Data Center facility; and b) the use of Mobile Broadband Modems on the PWGSC e-Procurement Solution Service Infrastructure.						
E2.21	Access Control	The Contractor must obtain PWGSC's approval for the use of external (i.e., non-Contractor) information systems for the delivery of PWGSC e-Procurement Solution Services.						
E2.22	Access Control	The Contractor must limit the use of Contractor-controlled portable storage media within the e-Procurement Solution Service (e.g., thumb drive) as follows: a) restrict the use to authorized Operators only, and b) restrict the use to PWGSC e-Procurement Solution Service Infrastructure components only.						
E2.23	Access Control	The Contractor must obtain PWGSC's approval before making any PWGSC e-Procurement Solution Service content publicly available.						
E2.24	Security Awareness and Training	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that includes operational roles and responsibilities for awareness and training.						
E2.25	Security Awareness and Training	The Contractor must provide security awareness and training for PWGSC e-Procurement Solution Service Infrastructure Operators as follows: a) as part of initial training for new Operators;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		b) before authorizing access to the PWGSC e-Procurement Solution Service Infrastructure or performing assigned duties, and c) annually or when security impacting changes to the e-Procurement Solution Service occur.						
E2.26	Security Awareness and Training	The Contractor must monitor and document e-Procurement Solution Service security awareness and training for PWGSC e-Procurement Solution Service Infrastructure Operators including: a) documenting who received what training course and when, and b) retaining records for the **last three (3) years**.						
E2.27	Audit and Accountability	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that include operational roles and responsibilities for audit and accountability.						
E2.28	Audit and Accountability	The e-Procurement Solution Service Identity Credential and Access Management Service must log the following events in accordance with the authentication event logging requirements for Level 3 Assurance, as detailed in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784). a) Successful authentication events; and b) unsuccessful authentication events.						
E2.29	Audit and Accountability	The Contractor must a) review and update the list of auditable events for e-Procurement Solution Service at minimum once in **180 Business Days**; b) include execution of privileged functions in the list of audit events; c) log events as identified and approved by PWGSC; and						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		d) automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.						
E2.30	Audit and Accountability	The Contractor must ensure that the e-Procurement Solution Service: a) produces audit records that t contain sufficient information, **as defined by PWGSC**, to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event; b) or audit events identified by type, location, or subject; and c) manages the content of audit records that are generated.						
E2.31	Audit and Accountability	The Contractor must perform capacity management on the e-Procurement Solution Service audit record storage by: a) allocating enough audit record storage capacity; b) configuring auditing to prevent storage capacity being exceeded; c) alerting the Operations Center when the allocated audit record storage volume r**eaches 75% of the audit record storage capacity**; and d) overwriting the oldest audit records if storage reached maximum capacity.						
E2.32	Audit and Accountability	The PWGSC e-Procurement Solution Service audit function must respond to auditing failures by: a) alerting the Operations Center; and b) overwriting the oldest audit records if storage reached maximum capacity.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.33	Audit and Accountability	The PWGSC e-Procurement Solution Service must use internal system clocks that are synchronized with an authoritative time source, approved by PWGSC, to generate time stamps for audit records.						
E2.34	Audit and Accountability	The PWGSC e-Procurement Solution Service must: a) protect audit information from unauthorized access, modification, and deletion; and b) backup audit records onto a different system or media than the system being audited on a schedule **as specified by PWGSC**.						
E2.35	Security Assessment and Authorization	The Contractor must develop an e-Procurement Solution Service vulnerability mitigation plan approved by PWGSC **within five (5) Business Days** of completion of a vulnerability assessment that includes proposed protection measures to mitigate the risks identified from the vulnerability assessment.						
E2.36	Configuration Management	The Contractor must develop, document, and maintain under configuration control, a current baseline configuration of the PWGSC e-Procurement Solution Service Infrastructure components and the **two (2) previous versions**.						
E2.37	Configuration Management	The Contractor must only allow authorized software, as documented by the Contractor and approved by PWGSC, to execute on the PWGSC e-Procurement Solution Service.						
E2.38	Configuration Management	The Contractor must a) plan, test the implementation of new and changed software, hardware and documentation for a PWGSC e-Procurement Solution Service release not using the production environment or						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		the control test environment of the PWGSC e-Procurement Solution Services; b) implement new and changed software, hardware and documentation for a PWGSC e-Procurement Solution Service release as approved by PWGSC; and c) develop and implement procedures for the distribution, installation, and rollback of changes implemented for a PWGSC e-Procurement Solution Service release.						
E2.39	Configuration Management	The Contractor must assess the security impact of changes by: a) analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; b) informing PWGSC of potential security impacts prior to change implementation, and c) checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements.						
E2.40		The Contractor must conduct audits of information system changes **at least every 12 months** and when indications so warrant determining whether unauthorized changes have occurred.						
E2.41	Configuration Management	The Contractor must review PWGSC e-Procurement Solution Service infrastructure Operator privileges on an annual basis.						
E2.42	Configuration Management	The Contractor must manage configuration settings for PWGSC e-Procurement Solution Service Infrastructure that includes: a) specifying configuration settings to implement least						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		privilege/functionality; b) documenting exceptions to configuration settings; and c) monitoring and controlling changes to the configuration settings in accordance with the Change Management and Configuration Management processes.						
E2.43	Configuration Management	The Contractor must employ automated mechanisms to centrally manage, apply, and verify configuration settings and to respond to unauthorized configuration changes by creating a Security Incident Ticket.						
E2.44	Configuration Management	The Contractor must open a security Incident Ticket when an unauthorized configuration change is detected in the e-Procurement Solution Service.						
E2.45	Configuration Management	The Contractor must configure the PWGSC e-Procurement Solution Service to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services **as approved by PWGSC**.						
E2.46	Configuration Management	The Contractor must develop, document, and maintain an inventory of the PWGSC e-Procurement Solution Service components that: a) accurately reflects their current configuration; b) is at the level of granularity deemed necessary for tracking and reporting; c) includes enough information to achieve effective property accountability; d) is available for review and audit by PWGSC; and e) is updated as an integral part of component installations, removals, and PWGSC e-Procurement Solution Service updates.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.47	Configuration Management	The Contractor must provide PWGSC with a change management process that includes measures used to enforce only authorized changes as applicable to the e-Procurement Solution Service.						
E2.48		The Contractor must employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of PWGSC e-Procurement Solution Service Infrastructure components that: a) detect the addition of unauthorized components into the PWGSC e-Procurement Solution Service Infrastructure, and b) create a Security Incident Ticket.						
E2.49	Configuration Management	The Contractor must provide a e-Procurement Solution Service Configuration Management Plan that: a) addresses roles, responsibilities, and configuration management processes and procedures; b) defines the Configuration Items for PWGSC e-Procurement Solution Services and when the Configuration Items are placed under configuration management; c) establishes the means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items; d) defines the processes for patch management on custom software utilized within the PWGSC e-Procurement Solution Service Infrastructure that includes: i) identifying, reporting, and correcting flaws in custom software; ii) testing software updates related to flaw remediation for effectiveness and potential side effects on the e-Procurement Solution Service before installation;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		iii) incorporating flaw remediation into the e-Procurement Solution Service configuration management process; e) defines the processes for patch management of the PWGSC e-Procurement Solution Service Infrastructure components that includes: i) ensuring the latest version of applications and operating systems are used; ii) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; iii) prioritizing critical patches using a risk-based approach; iv) taking applications offline and bringing them back online; v) aligning criticality levels for patches as specified by PWGSC; vi) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; vii) testing and verification methodology to ensure that patches have been implemented properly; and viii) notifying PWGSC of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of PWGSC e-Procurement Solution Service.						
E2.50		The Contractor must provide PWGSC with a e-Procurement Solution Service change management process that includes: a) Contractor's change management authorities; b) Contractor resource roles and responsibilities for change management; c) how The Contractor will use the change management process to support the development of the PWGSC e-Procurement Solution Services (e.g., a concept of operation); d) method used to uniquely identify configuration items; e) configuration item identification method; f) means for identifying Configuration Items throughout the						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		system development life cycle and a process for managing the configuration of the Configuration Items;						
E2.51	Contingency Planning	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that include operational roles and responsibilities for contingency planning.						
E2.52	Contingency Planning	The Contractor must coordinate the development and testing of the Service Continuity Plan with the organizational groups, within the Contractor and PWGSC, responsible for related plans.						
E2.53		The Contractor must conduct capacity planning so that necessary capacity for e-Procurement Solution Service processing, telecommunications, and environmental support exists during contingency operations.						
E2.54		The Contractor must train its personnel in their contingency roles and responsibilities with respect to the e-Procurement Solution Service, including simulated events to facilitate effective response in crisis situations, and provide refresher training at least annually.						
E2.55	Contingency Planning	The Contractor must work in conjunction with PWGSC to establish national restoration priorities for PWGSC e-Procurement Solution Services in an order of precedence **as specified by PWGSC.**						
E2.56	Contingency Planning	The Contractor must a) test the backup data for PWGSC e-Procurement Solution Services monthly to verify media reliability and data integrity; and b) use a sample of backup data for PWGSC e-Procurement Solution Services in the restoration of selected PWGSC e-						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		Procurement Solution Service functions as part of service continuity plan testing.						
E2.57	Contingency Planning	The Contractor must store backup copies of operating system software, critical system software, and component inventory in a separate facility or fire-rated container that is not collocated with the PWGSC e-Procurement Solution Service Infrastructure.						
E2.58	Contingency Planning	The Contractor must transfer any e-Procurement Solution Service backup data **within 24 hours of the backup being done to an alternate storage site.**						
E2.59	Contingency Planning	The Contractor must restore the PWGSC e-Procurement Solution Services to a known state after a disruption, compromise, or failure.						
E2.60	Contingency Planning	The Contractor must refresh the disk images of PWGSC e-Procurement Solution Service components from configuration-controlled and integrity-protected disk images.						
E2.61	Identification and Authentication	The Contractor must provide PWGSC with the operational security procedures that includes operational roles and responsibilities for identification and authentication requirements specified in this SOW.						
E2.62	Identification and Authentication	The PWGSC e-Procurement Solution Service must a) uniquely identify and authenticate Operators (or processes acting on behalf of Operators). b) issue user name and password credentials for Accounts that comply with the requirements for **Level 2 Assurance** as described in ITSG-31 (https://www.cse-cst.gc.ca/en/node/267/html/22784						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		). c) allow challenge/response questions for password recovery; d) allow one-time temporary passwords for enrolment and password recovery; e) allow one-time temporary passwords must be subject to a configurable validity period, as specified by PWGSC; f) allow one-time temporary passwords must be sufficiently random so as to not be predictable as approved by PWGSC; g) allow automatic advanced notification of pending password expiry as specified by PWGSC; h) allow password recovery policies and processes; and i) authenticate all Software Client access to the PWGSC e-Procurement Solution Service.						
E2.63	Identification and Authentication	The PWGSC e-Procurement Solution Service Identity Credential and Access Management Service must allow the binding and un-binding of one or more credentials to an individual Account. (e.g., an individual could use their PWGSC e-Procurement Solution **Level 2 credential** to access the PWGSC e-Procurement Solution Service as a User and use an additional X.509 credential to access the PWGSC e-Procurement Solution Service for administrative functions.).						
E2.64	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must c) enforce two-factor authentication using hard crypto token for all Operator accounts in compliance with CSE ITSG-31(https://www.cse-cst.gc.ca/en/node/267/html/22784); and d) perform mutual authentication of Operators Portable Devices connected to the network and only accept authorized Operators Portable Devices.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.65	Identification and Authentication	The Contractor must manage PWGSC e-Procurement Solution Service Infrastructure Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the PWGSC e-Procurement Solution Service Infrastructure and specifying access privileges; d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) notifying account administrator when temporary accounts are no longer required and when PWGSC e-Procurement Solution Service Infrastructure Operators are terminated, transferred, or PWGSC e-Procurement Solution Service Infrastructure usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year; k) deactivating: i) temporary accounts that are no longer required; ii) accounts of terminated or transferred Operators; iii) accounts after a number of day of inactivity as specified by PWGSC, and iv) temporary and emergency accounts over a given age; l) granting access to the PWGSC e-Procurement Solution Service Infrastructure based on: i) a valid access authorization;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		ii) intended system usage, and iii) other attributes as required by The Contractor or PWGSC; m) reviewing accounts at least monthly; n) locking the account after 10 unsuccessful login attempts occurring within 5 minutes, and o) keeping the account locked until manually unlocked by another Operator.						
E2.66		The PWGSC e-Procurement Solution Service Identification Credential and Access Management service must log the following events: a) account creation; b) account modifications c) account disabling, d) account termination; e) for Level 3 Assurance, as detailed in ITSG-31: i) password changes; ii) credential registrations; iii) password recovery; iv) expired credentials						
E2.67		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible.						
E2.68	Identification and Authentication	The PWGSC e-Procurement Solution Service Identity Credential and Access Management Service must automatically provision 1) Accounts for User e-Procurement Accounts and Generic Accounts, as follows: a) assign a unique e-Procurement Account and Display Name in accordance with the standard defined in subsection , by applying						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		configurable naming and conflict resolution rules; b) create an Account with no privileges; c) assign a one-time temporary password to the Account; d) create a Mailbox for the Account (if necessary); e) assign Account attributes and security access privileges as specified by PWGSC; and f) return the assigned e-Procurement Email Address, Display Name, Partner Unique Key, Contractor Unique Key and one-time password to the Account Requester.						
E2.69	Identification and Authentication	The Contractor designated registration authority must provide e-Procurement Solution Service Operator identifiers and authenticators (e.g., username, password, cryptographic token, etc.) in person to the authorized Operator.						
E2.70	Identification and Authentication	The Contractor must require multiple forms of physical identification be presented by an Operator for PWGSC e-Procurement Solution Services to a Contractor registration authority before the Operator receives identifiers and authenticators to access the PWGSC e-Procurement Solution Service Infrastructure.						
E2.71	Identification and Authentication	The Contractor must manage user authenticators for Operators by: a) verifying, as part of the initial authenticator distribution, the identity of the individual receiving the authenticator; b) establishing initial authenticator content for authenticators defined by the Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		d) establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon PWGSC e-Procurement Solution Service Infrastructure component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing/refreshing authenticators at a frequency not exceeding 180 days; h) protecting authenticator content from unauthorized disclosure and modification, and i) requiring Operators to take specific measures to safeguard authenticators.						
E2.72		The Contractor must manage device authenticators by: a) verifying, as part of the initial authenticator distribution, the identity of the device receiving the authenticator; b) establishing initial authenticator content for authenticators defined by The Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon PWGSC e-Procurement Solution Service Infrastructure component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing/refreshing authenticators at a frequency not exceeding 180 days;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		h) protecting authenticator content from unauthorized disclosure and modification, and i) having devices implement specific measures to safeguard authenticators.						
E2.73		The PWGSC e-Procurement Solution Service authentication process for X.509 credentials must include: a) performing path validation of the X.509 certificate; and b) checking the revocation status of the X.509 certificate.						
E2.74	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must, for password-based authentication: a) enforce minimum password complexity of **case sensitive, 15 characters, with at least one upper case, one lower case, one number, and one special character**; b) encrypt passwords in storage and in transmission; c) enforce password **maximum lifetime of 90 days**, and d) prohibit password **reuse for 10 generations**.						
E2.75		The PWGSC e-Procurement Solution Service Identity Credential and Access Management Service must provide a) the User with a checklist that presents the rules a password must comply with and check these rules positively as they are satisfied when the User enters the password. b) configurable User password rules as specified by PWGSC that include: i) minimum number of total characters; ii) minimum number of uppercase and lowercase characters; ii) minimum number of numeric characters; iv) minimum number of non-alpha-numeric characters; v) words found in dictionary (English and French);						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		vi) password re-use history; vii) maximum lifetime of the password.						
E2.76	Identification and Authentication	The Contractor must require that the registration process for PWGSC e-Procurement Solution Service Operators to receiver identifiers and authenticators be carried out in person before a designated registration authority with authorization by a designated Contractor's official (e.g., a supervisor).						
E2.77	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must not transmit clear text passwords over any network.						
E2.78	Identification and Authentication	The Contractor must not allow unencrypted static authenticators to be embedded in PWGSC e-Procurement Solution Service Infrastructure applications or access scripts or stored on function keys.						
E2.79	Identification and Authentication	The PWGSC e-Procurement Solution Service Infrastructure must obscure feedback of Operator authentication data (e.g., masking password fields) during the authentication process.						
E2.80	Identification and Authentication	The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the PWGSC e-Procurement Service have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		maintenance personnel do not possess the required access authorizations.						
E2.81	Incident Response	1) The Contractor must provide PWGSC with the operational security procedures that includes operational roles and responsibilities for Incident response requirements specified in this SOW.						
E2.82		The Contractor must implement and test the service continuity plan (all processes, procedures, roles, responsibilities etc) on an annual basis, and provide the test results to PWGSC **within ten (10) Business Days** of completion of the service continuity plan testing.						
E2.83		The Contractor must provide a service continuity plan (SCP) to PWGSC that includes: a) detailed plan and documented processes for restoring PWGSC e-Procurement Solution Services; b) details the communications plan with PWGSC and its suppliers; c) details plan and processes for transferring operational, management and administration functionality to a backup operations centre; d) back up strategies for datacenter facilities, network facilities, operational support systems and data, and key service components; e) how The Contractor will ensure that its suppliers have in place service continuity plans; f) describes the process for testing the Service Continuity Plan; g) steps The Contractor will take if any of its key suppliers go out of business, and h) steps The Contractor will take if any of its manufacturers or						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		Original Equipment Manufacturers (OEM) is no longer considered a trusted manufacturer or OEM by PWGSC.						
E2.84		The Contractor must provide a final version of the Service Continuity Plan **within 15 Business Days** after receiving comments from PWGSC on the draft Service Continuity Plan.						
E2.85		The Contractor must implement the Service Continuity Plan (all processes, procedures, roles, responsibilities etc.), and any subsequent annual updates, **within 60 Business Days** following acceptance by PWGSC.						
E2.86		The Contractor must provide to PWGSC **within 40 Business Days** of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the Service Continuity Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting PWGSC's service continuity requirements.						
E2.87		If The Contractor determines that it will take more than 40 Business Days to provide the requested evidence for the Service Continuity Plan, The Contractor must notify PWGSC **within five (5) Business Days** of the original request for evidence, and request an extension, in writing with appropriate justification. Granting an extension is within PWGSC's sole discretion.						
E2.88		The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.89		In addition to any sources of intelligence on cyber threats and Incidents sources that The Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).						
E2.90		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.						
E2.91		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.						
E2.92		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		c) security Incident handling and response; and d) auditing.						
E2.93		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.						
E2.94		The Contractor must automatically provide Incident Ticket information by secure e-mail to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.95		The Contractor must continue to automatically send secure e-mail upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.96		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada’s priority level.						
E2.97		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.						
E2.98		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible						
E2.99		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.						
E2.100	Incident Response	The Contractor must provide training for PWGSC e-Procurement Solution Service Infrastructure Operators in their security Incident response roles and responsibilities and provide annual refresher training.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.101		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.102		The Contractor must continue to automatically send e-Procurement upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.103		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.						
E2.104		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.						
E2.105		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible.						
E2.106		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.						
E2.107	Incident Response	The Contractor must test the Incident response process for the e-Procurement Solution Service at least annually using comprehensive test scripts to determine the Incident response effectiveness including: a) documenting the test results; b) reviewing the test results with PWGSC, and c) implement corrective actions as required by PWGSC within a timeframe agreed to with PWGSC.						
E2.108	Incident Response	The Contractor must ensure that the security posture of the PWGSC e-Procurement Solution Services is maintained by continuously: a) monitoring threats and vulnerabilities; b) monitoring for malicious activities and unauthorized access;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		and c) where required, taking proactive countermeasures, including taking both pre-emptive and response actions to mitigate threats.						
E2.109		The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance.						
E2.110		In addition to any sources of intelligence on cyber threats and Incidents sources that the Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).						
E2.111		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.						
E2.112		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.						
E2.113		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.						
E2.114		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination. (The SOC must use a Secure Terminal Equipment (STE), provided as Government Furnished Equipment, following existing COMSEC processes, to communicate with PWGSC when requested by PWGSC that includes a unique and dedicated telephone number.						
E2.115		The SOC must accept e-mails from PWGSC authorized representatives to a Contractor-provided mailbox with an auto reply to confirm receipt of the e-mail.						
E2.116		The SOC must acknowledge receipt of e-Procurements received from e-Procurement addresses authorized by PWGSC **within 15 minutes** of receiving the e-Procurement 24 hours per day, 7 days per week, and 365 days per year.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.117		The SOC must authenticate the identity of the requester using a process approved by PWGSC						
E2.118		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.119		The Contractor must continue to automatically send e-mail upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.120		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.						
E2.121		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.						
E2.122		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible						
E2.123		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.						
E2.124		The Contractor must create one or more Incident Tickets for each Incident detected by The Contractor or reported by PWGSC.						
E2.125		The Contractor must physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in PWGSC dedicated storage.						
E2.126		The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and PWGSC-reported Incidents.						
E2.127		The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.128	Incident Response	The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements files) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.						
E2.129		The Contractor must create an Emergency Change Request, within a time period specified by PWGSC, for each mitigation measure requested by PWGSC to contain a Security Incident.						
E2.130		The Contractor must create an Emergency Change Request, based on severity as specified by PWGSC, for each mitigation measure requested by PWGSC to contain a Security Incident and, must implement the Emergency Change Request in accordance with PWGSC's priority level.						
E2.131	Incident Response	The Contractor must a) revise the severity level and priority of an Incident when requested to do so by PWGSC within 15 minutes of the request; b) automatically escalate Incidents according to escalation levels and time periods specified by PWGSC; c) provide PWGSC with an operational escalation matrix and a management escalation matrix that defines the personnel, with alternates (of equal authority) for a minimum of 5 Escalation Levels (Escalation Level 1 to Escalation Level 5, where Escalation Level 5 is the most senior personnel), and contains clear contact instructions; d) provide PWGSC with notification of Incidents according to the operational and management escalation matrices; and e) classify, assign and escalate Incidents for Incident resolution based on priority in accordance with severity and impact levels as specified by PWGSC.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.132	Incident Response	The Incident Tickets for Security Incidents must include, the following additional information: a) type and description of attack/event; b) whether attack appears to have been successful and impact; c) attack scope (to an organization and/or across many organizations); d) estimated number of systems affected by organization; e) list of systems affected by organization; f) apparent source/origin of attack/Incident/event; g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration; k) actions taken; l) status of mitigations, and m) applicable logs or evidence data.						
E2.133		The Contractor must automatically provide Incident Ticket information by Email to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.134		The Contractor must continue to automatically send Email upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.135		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures,						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.						
E2.136		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.						
E2.137		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible.						
E2.138		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		the PWGSC e-Procurement Solution Service. The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.						
E2.139		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.						
E2.140		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.						
E2.141		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include:						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.						
E2.142	Incident Response	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance.						
E2.143		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.						
E2.144		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.						
E2.145		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.						
E2.146		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.						
E2.147		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.148		The Contractor must continue to automatically send e-Procurement upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.149		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities,						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.						
E2.150		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible						
E2.151		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.						
E2.152		Add these items to the Security Incident Ticket: g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration;						
E2.153		The Contractor must report all suspected or actual privacy and security violations for PWGSC e-Procurement Solution Services as Security Incidents.						
E2.154		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.155		The Contractor must provide all evidence, in a COTS format specified by PWGSC, associated to a Security Incident, within a time interval specified by PWGSC that includes: a) results of historical logs and audit records research associated with one or many Partners based on criteria provided by PWGSC; b) results of analysis of logs and audit records associated with one or many organizations based on criteria provided by PWGSC; c) logs and audit records based on criteria provided by PWGSC, and d) additional information or data as specified by PWGSC.						
E2.156		The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and PWGSC-reported Incidents.						
E2.157		The Contractor must update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.						
E2.158		The Contractor's Incident Tickets must include and maintain, but not be limited to, the following dedicated information fields for all Incidents: a) Contractor's Ticket number; b) Incident description; c) Incident originator contact information (name, telephone number and e-Procurement address); d) Incident originator language; e) related Incident Tickets; f) date and time stamp when Incident Tickets initiated; g) date and time stamp when Incident Ticket closed; h) Incident Ticket type; type (e.g. production, functional testing, performance testing, security, etc.) as specified by PWGSC;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		i) Incident Ticket severity; j) Incident Ticket impact; k) Incident Ticket priority; l) Incident Ticket status (i.e. open, closed, in progress, suspended, cancelled etc.); m) Incident Ticket escalations;<TRACEFROM>SR-599</TRACEFROM> n) PWGSC's ticket number; o) Service functions impacted; p) affected Service Delivery Points; q) Contractor contact (name, telephone number and e-Procurement address); r) Partner identifier (If applicable); s) Interactions with third parties;<TRACEFROM>SR-599</TRACEFROM> t) activity log; u) root cause (if available); v) estimated time for resolution (updated every 15 minutes); w) resolution description and x) outage time (for closed tickets only).						
E2.159		The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and PWGSC-reported Incidents.						
E2.160		The Contractor must update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.						
E2.161		The Contractor must notify PWGSC via phone and e-Procurement (7 days x 24 hours x 365 days), based on priority as specified by PWGSC, of any suspected or actual Security Incidents, including: ii) denial of service attacks; iii) malware;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		iv) social engineering; v) unauthorized intrusion or access; vi) information breach; and vii) all other security breaches or cyber threats targeting Canada.						
E2.162		The Contractor must not withhold from PWGSC any information or data in its possession that relates to PWGSC e-Procurement Solution or is associated with a Security Incident.						
E2.163		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.						
E2.164		The Contractor must provide a secure Security Management Portal that will allow Canada to view security-related information within the PWGSC e-Procurement Solution Service. This includes but is not limited to: a) security Incident reports, post-mortem, adhoc reports, and associated evidence; b) security Incident tickets; c) user activity reports; d) operator activity reports;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		e) access reports; f) configuration audit reports; g) configuration change reports; h) file integrity monitoring reports; i) inventory reports; j) vulnerability reports; k) configuration change reports; l) Emergency Request For Changes and Request For Changes; m) patches and security patches implemented; n) information on whether specific e-Procurements are being blocked/filtered and for how long; and o) other supporting documentation (e.g. whitelisting, blacklisting).						
E2.165		The Contractor must report all suspected or actual privacy and security violations for PWGSC e-Procurement Solution Services as Security Incidents.						
E2.166		The Contractor must report all suspected or actual privacy and security violations for PWGSC e-Procurement Solution Services as Security Incidents.						
E2.167	Incident Response	The Contractor must provide a Monthly Management Report (MMR) that includes: a) executive overview; b) summary of Incident activity; c) summary of security Incidents and remedial actions taken; and d) summary of patches and security patches implemented.						
E2.168		The Contractor must provide a monthly security threat report to PWGSC that includes: a) top 25 threat vectors; b) top 25 targeted service/protocol/applications; c) top 10 origin/source of attack; and d) top 25 types of attacks (e.g. injection, phishing, DoS, cross-site scripting, drive-by downloading, etc.).						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.169		The Contractor must provide a monthly report to Canada of all Security Incidents that includes the following information: a) Incident Ticket number; b) Incident Ticket opened/closed date; c) threat vector; d) targeted service/protocol/application; e) origin/source of attack, and f) type of attack (e.g. injection, phishing, DoS, cross-site scripting, drive-by downloading, etc.).						
E2.170		The Contractor must provide a security breach report weekly and when requested by PWGSC that includes: a) number of Security Incidents; b) number of security investigations completed; c) average/highest response time to Security Incidents, and d) average/highest security investigation completion time.						
E2.171		The Contractor must provide a security breach report weekly and when requested by PWGSC that includes: a) number of Security Incidents; b) number of security investigations completed; c) average/highest response time to Security Incidents, and d) average/highest security investigation completion time.						
E2.172		The SOC must provide the service of a Security Operations and Response Specialist who will be PWGSC's point of contact for: a) Security Incidents; b) security issues; c) requests for information on security; d) coordination of security response, and e) security alerts.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.173		The Security Operations and Response Specialist must have the following minimum qualifications: a) have relevant experience in security operations and response; b) have in-depth knowledge of the PWGSC e-Procurement Solution; c) be capable of rapidly analyzing and assessing Incident data; d) be capable of providing a factual assessment of the situation; e) be fully trained on the PWGSC e-Procurement Solution security monitoring and reporting solution; f) be capable of rapidly responding to inquiries; g) be client oriented; h) be capable of working under high stress and pressure, and i) be bilingual.						
E2.174	Incident Response	Meetings for Security Incidents, or security related matters as identified by PWGSC, must be in Person in the National Capital Region (NCR) during business hours (08:00 to 17:00 ET) Monday to Friday and during hours outside that time period as agreed to between The Contractor and PWGSC.						
E2.175		The Contractor must be available to participate in a Security Incident briefing provided by Canada, (e.g. for Classified briefing).						
E2.176	Incident Response	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance. In addition to any sources of intelligence on cyber threats and Incidents sources that The Contractor monitors in its routine operations, The Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).						
E2.177		The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase 1, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of PWGSC e-Procurement Solution Security Incidents.						
E2.178		The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with PWGSC; b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) act as a point of contact for communications with PWGSC representatives for security incidents; d) not impact operations of PWGSC e-Procurement Solution Services in case of a Contractor SOC failure; e) notify PWGSC within 15 minutes if Contractor SOC is not available and provide contact name PWGSC can communicate as necessary during The Contractor SOC outage.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.179		The SOC must work with PWGSCs Information Protection Centre for activities that include: a) integration of processes; b) oversight; c) Security Incident handling and response; and d) auditing.						
E2.180		The SOC must work with the PWGSC IPC and PWGSC's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery that include: a) ability to dispatch the ITSIRT to The Contractor site; and b) allowing PWGSC to provide on-site guidance and coordination.						
E2.181		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.182		The Contractor must continue to automatically send e-Procurement upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.183		The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious e-Procurements) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.184		The Contractor must provide a Security Incident post-mortem report to PWGSC, within 72 hours of a request by PWGSC, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with PWGSC e-Procurement Solution Service, and j) recommendations to improve PWGSC e-Procurement Solution Service.						
E2.185		The PWGSC e-Procurement Solution Service Infrastructure must record in the audit logs, at a minimum, and at all PWGSC e-Procurement Solution Service Infrastructure components where feasible						
E2.186		The Contractor must monitor on a continuous basis events on the PWGSC e-Procurement Solution Service Infrastructure to: a) detect attacks, Incidents and abnormal events against the PWGSC e-Procurement Solution Service and the Infrastructure; b) identify unauthorized use and access of PWGSC e-Procurement Solution Data and PWGSC e-Procurement Solution Service Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the PWGSC e-Procurement Solution Service.						
E2.187		The Contractor must automatically provide Incident Ticket information by e-Procurement to a pre-defined distribution list for each PWGSC e-Procurement Solution Service for Incidents where						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		PWGSC specifies: a) information from Incident Ticket; b) frequency of e-Procurement updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).						
E2.188		The Contractor must continue to automatically send Email upon updates of Incidents until the Incident is closed or PWGSC cancels the automatic update reporting for the Incident.						
E2.189		The Contractor must have proper forensic procedures and safeguards in place that includes: a) the maintenance of a chain of custody for both the audit information, and b) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.						
E2.190		The Contractor must develop an incident response plan that includes: a) how The Contractor plans to identify, report, and escalate Security Incidents; b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery; c) a description of the structure and organization of the Security Incident response capability; d) a high-level approach for how the Security Incident response capability fits into The Contractor's overall organization; e) a definition of reportable Security Incidents; f) a definition of metrics for measuring the Security Incident response capability; and g) a definition of resources and management support needed to						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		effectively maintain and mature the Security Incident response capability.						
E2.191	System Maintenance	The Contractor must perform controlled maintenance by: a) scheduling, performing, documenting, and reviewing records of maintenance and repairs on PWGSC e-Procurement Solution Service Infrastructure components in accordance with manufacturer or vendor specifications; b) controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location; c) requiring that a designated Contractor's official explicitly approve the removal of the PWGSC e-Procurement Solution Service Infrastructure components from The Contractor data centre for off-site maintenance or repairs; d) sanitizing equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, and e) checking all potentially impacted security requirements to verify that the controls are still functioning properly following maintenance or repair actions.						
E2.192	System Maintenance	The Contractor must approve, control, monitor and maintain, on an ongoing basis, the hardware and software used for maintaining the PWGSC e-Procurement Solution Service Infrastructure specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).						
E2.193	System Maintenance	The Contractor must a) check all media containing diagnostic and test programs for						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		malicious code before the media are used on PWGSC e-Procurement Solution Service Infrastructure components; b) verifying that there is no PWGSC e-Procurement Solution Service information contained on the equipment; c) sanitizing or destroying the PWGSC e-Procurement Solution Service equipment; d) retaining the PWGSC e-Procurement Solution Service equipment within the PWGSC e-Procurement Solution Service facility or obtaining an exemption from a designated PWGSC e-Procurement Solution Service Contracting Authority explicitly authorizing removal of the equipment from the PWGSC e-Procurement Solution Service facility.						
E2.194	System Maintenance	The Contractor must authorize, monitor, and control maintenance and diagnostic activities on the PWGSC e-Procurement Solution Service Infrastructure by: a) allowing the use of maintenance and diagnostic tools approved by PWGSC; (to be discussed) b) employing strong identification and authentication techniques in the establishment of maintenance and diagnostic sessions that tightly bound to the user and by separating the maintenance session from other network sessions with the PWGSC e-Procurement Solution Service Infrastructure by either: (i) physically separated communications paths; or (ii) logically separated communications paths using CSE-approved cryptographic modules and algorithms (see subsection Encryption Standards); c) recording maintenance and diagnostic sessions; and d) having designated personnel review the records of the maintenance and diagnostic sessions.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.195	System Maintenance	The Contractor must: a) sanitize equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, b) inspect and sanitize components (with regard to potentially malicious software and surreptitious implants), that have been serviced off-site before reconnecting the component to the PWGSC e-Procurement Solution Service Infrastructure; c) protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either: (i) Physically separated communications paths; or (ii) Logically separated communications paths based upon encryption compliant with the requirements of control SC-13. d) Maintenance personnel notify [Assignment: organization-defined personnel] when non-local maintenance is planned (i.e., date/time); e) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance; f) employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communication; and g) employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.						
E2.196	System Maintenance	The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the e-Procurement Solution Service have required access						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		authorizations; and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.						
E2.197	Media Protection	The Contractor must provide PWGSC with the operational security procedures that includes media protection requirements specified in this SOW.						
E2.198	Media Protection	The Contractor a) must restrict access to IT media (digital and non-digital) containing PWGSC e-Procurement Solution Data to authorized Operators; and b) employ mechanisms to audit access attempts and access granted.						
E2.199	Media Protection	The Contractor must mark, in accordance with the provisions of the contract, removable IT media containing Canada information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.						
E2.200	Media Protection	The Contractor must: a) physically control and securely store IT media containing PWGSC e-Procurement Solution Data in accordance with the RCMP G1-001, Security Equipment Guide; and b) physically control and securely store IT media containing PWGSC e-Procurement Solution Data awaiting destruction (either on- or off-site) using PWGSC approved equipment, techniques, and procedures.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.201	Media Protection	The Contractor must employ cryptographic mechanisms to protect information in storage that are approved by PWGSC and are in compliance with CSE guidance (ITSG-111).						
E2.202	Media Protection	The Contractor must sanitize and verify IT media containing PWGSC e-Procurement Solution Data, both digital and non-digital, prior to disposal, release out of The Contractor's control, or release for reuse.						
E2.203	Media Protection	The Contractor must track, control and verify media sanitization by: a) performing media sanitization in compliance with ITSG-06 (http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-eng.html) requirements for Secret information; b) recording media sanitization actions; c) testing sanitization equipment and procedure to verify correct performance at least annually; and d) sanitizing re-allocated used storage devices prior to connecting them to the PWGSC e-Procurement Service Infrastructure						
E2.204	Physical and Environmental Protection	The Contractor must provide PWGSC with the operational security procedures that includes physical and environmental protection requirements specified in this SOW.						
E2.205	Physical and Environmental Protection	The Contractor must implement role-based physical access control to its PWGSC e-Procurement Solution Service Infrastructure facilities including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access PWGSC e-Procurement Solution Service Infrastructure; g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access; and h) keeping the management of The Contractor's physical access control authorizations to the PWGSC e-Procurement Solution Service Facility independent of the physical access control authorization to the facility where the PWGSC e-Procurement Solution Service Facilities are located. i) If emergency access is required, contact the RCMP for advice.						
E2.206	Physical and Environmental Protection	The Contractor must implement role-based physical access control to its PWGSC e-Procurement Solution Service Infrastructure facilities including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access PWGSC e-Procurement Solution Service Infrastructure; g) allowing access to facilities to authorized personnel based on a						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		need-to-know and need-to-access; h) keeping the management of The Contractor's physical access control authorizations to the PWGSC e-Procurement Service Facility independent of the physical access control authorization to the facility where the PWGSC e-Procurement Service Facilities are located; and i) If emergency access is required, contact the RCMP for advice.						
E2.207	Physical and Environmental Protection	The Contractor must provide PWGSC with a building security plan for review by PWGSC including: a) physical security layout for access control points; b) physical security zones; c) monitoring physical access points; and d) The Contractor must enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the infrastructure resides (excluding those areas within the facility officially designated as publicly accessible); i) Verify individual access authorizations before granting access to the facility; ii) Controls entry to the facility containing the infrastructure using physical access devices and/or guards; iii) Control access to areas officially designated as publicly accessible in accordance with The Contractor's assessment of risk; iv) Secure keys, combinations, and other physical access devices; v) Inventories physical access devices at least annually; and vi) Combinations and keys must be changed immediately when keys are lost, combinations are compromised, or individuals are transferred or terminated.						
E2.208	Physical and Environmental Protection	The Contractor must monitor physical access to PWGSC e-Procurement Solution Service Infrastructure facilities by: a) monitoring in real-time physical intrusion alarms and						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		surveillance equipment; b) recording all physical access events; c) reviewing physical access logs at least monthly; d) providing logs on a monthly basis and as requested by PWGSC; and e) create a Security Incident upon discovery of abnormal activity.						
E2.209	Physical and Environmental Protection	The Contractor must control physical access to PWGSC e-Procurement Solution Service Infrastructure facilities by: a) authenticating visitors before authorizing access with PWGSC approval to the facility where the infrastructure resides; b) authenticating visitors with two forms of identification prior to granting access to the PWGSC e-Procurement Solution Service facility; and c) escorting visitors and monitoring visitor activity, within the PWGSC e-Procurement Solution Facility at all times.						
E2.210	Physical and Environmental Protection	The Contractor must review visitor access records for the PWGSC e-Procurement Solution Facility **at least every 90 days**.						
E2.211	Physical and Environmental Protection	The Contractor must protect power equipment and power cabling servicing the PWGSC e-Procurement Solution Facility from damage and destruction.						
E2.212	Physical and Environmental Protection	The Contractor must implement protection devices to prevent the accidental activation of emergency power shutoff mechanisms of PWGSC e-Procurement Solution Service Infrastructure.						
E2.213	Physical and Environmental Protection	The Contractor must authorize, monitor, and control all components entering and exiting the PWGSC e-Procurement Solution Service Infrastructure facilities and maintain records of those components and activities. Records must be made available monthly and as requested by GC.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.214	Physical and Environmental Protection	The Contractor must a) implement at alternate work sites management, operational, and technical security controls that achieve the same objectives as those implemented at the main PWGSC e-Procurement Solution Facility. b) Alternate site must be approved concurrently with the Primary sites by CISD/IISD.						
E2.215	Personnel Security	The Contractor must, upon termination of an individual's employment associated with PWGSC e-Procurement Solution Services: a) terminate physical access to PWGSC e-Procurement Solution Service Infrastructure facilities for the employee; b) terminate PWGSC e-Procurement Solution Service Infrastructure access, including remote access, and c) retrieve all security-related property (e.g., employee identity card, physical authentication token).						
E2.216	Personnel Security	The Contractor must manage PWGSC e-Procurement Solution Service Infrastructure privileged Operators accounts as follows: a) create Operator accounts in accordance with role-based access profiles that specify privileges; b) track and monitor Operator role assignments, and c) adjust role assignments as Operator role changes.						
E2.217		The Contractor must implement role-based physical access control to its PWGSC e-Procurement Solution Service Infrastructure facilities including: a) keeping an access list of personnel with authorized access to the facilities; b) issuing authorization credentials for access to the facilities; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		d) authorizing physical access to the facilities, by access point, based on the role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access PWGSC e-Procurement Solution Service Infrastructure; g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access;, and h) keeping the management of The Contractor's physical access control authorizations to the Email Service Facility independent of the physical access control authorization to the facility where the Email Service Facilities are located. i) If emergency access is required, contact the RCMP for advice.						
E2.218	Personnel Security	The Contractor must have access agreements to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data where: a) prior to being granted access to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data, Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) The Contractor reviews and updates access agreements to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data every two years.						
E2.219	Personnel Security	The Contractor must a) prior to being granted access to the PWGSC e-Procurement Solution Service Infrastructure or PWGSC e-Procurement Solution Data, ensure that the Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) provide training for PWGSC e-Procurement Solution Service						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		Infrastructure Operators in their responsibilities to protect the privacy and confidentiality of the PWGSC e-Procurement Solution Data as per the terms and conditions of the PWGSC e-Procurement Solution contract and in the sanctions for failure to comply. The Contractor must provide bi-annual refresher training.						
E2.220	Risk Assessment	The Contractor must allow PWGSC, or its representatives, to conduct a Vulnerability Assessment against the PWGSC e-Procurement Solution Service, within 3 Federal Government Working Days of a request by PWGSC, that includes: a) physical access to the PWGSC e-Procurement Solution Service facilities (i.e. Contractor's facilities where the PWGSC e-Procurement Solution Service Infrastructure (i.e. hardware and software) is located); b) network access(es) to the PWGSC e-Procurement Solution Service Infrastructure to allow for authenticated and unauthenticated scanning of network components and security appliances, using PWGSC operated equipment, and PWGSC specified tools; c) assistance for the duration of any onsite portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the PWGSC e-Procurement Solution Service Infrastructure (i.e., the hardware, software, and network components, security appliances, and their configuration); (7) PWGSC will limit its Vulnerability Assessment to discovery and scanning activities to PWGSC e-Procurement Solution Service Infrastructure and will not engage in disruptive or destructive activities.						
E2.221	Risk Assessment	The Contractor must ensure that the network access (es) to the PWGSC e-Procurement Solution Service Infrastructure to allow for authenticated and unauthenticated scanning of network						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		components and security appliances, using PWGSC operated equipment, and PWGSC specified tools.						
E2.222	Risk Assessment	The Contractor must run automated vulnerability scanning tools against all PWGSC e-Procurement Solution Service Infrastructure components on a monthly basis, or as specified by PWGSC.						
E2.223	System and Services Acquisition	From the date vulnerabilities are formally identified, The Contractor must, at a minimum: a) Mitigate all high-risk vulnerabilities within 10 days; and b) Mitigate all moderate risk vulnerabilities within 30 days. PWGSC and Contractor will mutually agree and determine the risk rating of vulnerabilities.						
E2.224		The Contractor must maintain the Email Service's security authorization state through continuous monitoring and annual audit of the implemented security requirements within the e-Procurement Service to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the e-Procurement Service and its operational environment.						
E2.225		The Contractor must provide evidence to support authorization maintenance activities, within 30 days of a request by PWGSC, following all changes to the PWGSC e-Procurement Solution Service Infrastructure within The Contractor’s control.						
E2.226		The Contractor must update, as requested by PWGSC, and within 30 days of a request by PWGSC, security operating procedures and demonstrate implementation as part of authorization maintenance.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.227	System and Communications Protection	The Contractor as part of the Security Operational Procedures must include policy and procedures to facilitate the implementation and maintenance of the system and communications protection requirements specified in this SoR and in applicable GC standards specified in this SoR.						
E2.228	System and Communications Protection	The PWGSC e-Procurement Solution Service must include a Denial of Service (DoS) capability that limits concurrent connections as **specified by PWGSC**.						
E2.229	System and Communications Protection	1) The service design for PWGSC e-Procurement Solution Services must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (<insert URL link here>) and ITSG-38 (<insert URL link here>). Additionally, The PWGSC e-Procurement Solution Service Infrastructure must monitor and control communications at the external boundary of the system and at key internal boundaries within the system in compliance with ITSG-22 and ITSG-38. 2) The PWGSC e-Procurement Solution Service Contractor must monitor and analyze network traffic, in near real time, to detect attacks and evidence of compromised PWGSC e-Procurement Solution Service Infrastructure components. 3) The PWGSC e-Procurement Solution Service Contractor must detect attacks including but not limited to: a) denial of service attacks; b) malware; c) social engineering; d) unauthorized intrusion or access; e) information breach; and f) all other security breaches or cyber threats targeting Canada.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.230	System and Communications Protection	The PWGSC Contractor must a) physically allocate publicly accessible PWGSC e-Procurement Solution Service Infrastructure components to separate sub-networks with separate physical network interfaces; b) implement the Mobile Device Management (MDM) service in accordance with guidance in ITSG-22 and ITSG-38; c) implement the MDM mobile data service and connection service in its own separate physical network segment connected through a physical firewall appliance (<insert URL from CSE>) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. If this is not achievable The Contractor must obtain approval from PWGSC for alternate products; and d) implement the MDM Management Service attachment service in its own separate physical network segment connected through a physical firewall appliance (<insert URL from CSE>) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. If this is not achievable The Contractor must obtain approval from PWGSC for alternate products.						
E2.231	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must exclusively connect to external networks or information systems specified by Canada only through managed interfaces specified by Canada using boundary protection devices arranged in compliance with ITSG-22 and ITSG-38.						
E2.232	System and Communications Protection	The Contractor must actively manage all network connections to external services associated with the PWGSC e-Procurement Solution Service Infrastructure as follows: a) deny all network traffic by default;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by PWGSC; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.						
E2.233	System and Communications Protection	The Contractor must prevent Contractor managed devices (e.g.: notebook or other device used for administration) that are connected with the PWGSC e-Procurement Solution Service Infrastructure from communicating outside of that communications path (e.g. accessing the Internet via a separate connection available to the device).						
E2.234	System and Communications Protection	1) The PWGSC e-Procurement Solution Service Infrastructure must route internal network traffic to external networks through authenticated proxy servers as defined by PWGSC within the managed interfaces of boundary protection devices. 2) The PWGSC e-Procurement Solution Service Design must allow Mobile Device traffic to pass through a Canada Internet proxy **as specified by PWGSC**.						
E2.235	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must detect extrusion events in **near real time**.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.236	System and Communications Protection	The Contractor must monitor and analyze hosts behaviours (Host-based Intrusion Detection and Prevention) in near real-time to detect attacks and evidence of compromised hosts						
E2.237	System and Communications Protection	The Contractor must a) physically separate the network IP traffic of the PWGSC e-Procurement Solution System Data from the PWGSC e-Procurement Solution Service Management Data and PWGSC e-Procurement Solution Service User Data. b) Logically separate the network IP traffic between the PWGSC e-Procurement Solution Service Management Data and the PWGSC e-Procurement Solution User Data.						
E2.238	System and Communications Protection	The Contractor must configure boundary protections (i.e. firewall) to fail safe (i.e. no traffic goes through) upon failure.						
E2.239	System and Communications Protection	The PWGSC e-Procurement Solution Service Design a) must allow mutual authentication of connections, between the e-Procurement Solution Service and other domains as specified by PWGSC, and exclusively exchange information with these other domains using mutual authentication. b) Must ensure that the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC.						
E2.240	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure a) must protect the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards). unless otherwise protected by alternative physical measures approved by PWGSC; and						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		b) must protect the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards). unless otherwise protected by alternative physical measures approved by PWGSC.						
E2.241	System and Communications Protection	The PWGSC e-Procurement Solution Service Design must a) allow mutual authentication of connections, between the e-Procurement Service and other domains as specified by PWGSC, and exclusively exchange e-Procurement Messages with these other domains using mutual authentication; b) ensure that the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC; c) conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (<insert URL here>) and ITSG-38 (<insert URL here>); and d) encrypt Security Incident information with approved cryptographic standards (see subsection Encryption Standards) if the information is sent in electronic form.						
E2.242	System and Communications Protection	The Contractor must actively manage all network connections to external services associated with the PWGSC e-Procurement Solution Service Infrastructure as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by PWGSC; d) document each exception to the traffic flow policy with a						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.						
E2.243	System and Communications Protection	The PWGSC e-Procurement Solution Service Design must ensure that a) cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for PWGSC e-Procurement Solution Services: i) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSA-11E (http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-eng.html) or in a subsequent version; ii) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-eng.html) to at least FIPS 140-2 validation at Level 1, and iii) operate in FIPS Mode. b) the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC.						
E2.244	System and Communications Protection	The PWGSC e-Procurement Solution Service Design must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-eng.pdf) and						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		ITSG-38 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-eng.pdf).						
E2.245	System and Communications Protection	The Contractor must not prohibit a User to encrypt, decrypt, sign and verify PWGSC e-Procurement Solution attachment files using Certificates trusted by the GC-CA.						
E2.246	System and Communications Protection	The Contractor must only allow pre-approved mobile code in the PWGSC e-Procurement Solution Service Infrastructure thus denying any other mobile code from being downloaded and executed.						
E2.247	System and Communications Protection	The Contractor must prohibit the use of VoIP technologies in the PWGSC e-Procurement Solution Service Infrastructure unless specifically authorized by PWGSC.						
E2.248	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure component or components that collectively provide name/address resolution service for the PWGSC e-Procurement Solution Service must implement internal/external role separation.						
E2.249	System and Communications Protection	The PWGSC e-Procurement Solution Service must allow authentication of the following Software Client types with an X.509 credential using mutual transport layer authentication (TLS): a) Web Browser Clients; and b) Mobile Browser Clients.						
E2.250		The PWGSC e-Procurement Solution Service must allow the authentication of all types of Software Clients with a PWGSC e-Procurement Solution Service credential.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.251	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must invalidate session identifiers upon operator logout or other session termination.						
E2.252	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must use a readily observable logout capability whenever authentication is used to gain access to PWGSC e-Procurement Solution Service Infrastructure components.						
E2.253	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must a) generate a unique session identifier for each session with randomness using CSE-approved cryptography (see subsection Cryptographic Standards); and b) recognize only session identifiers that are generated by the PWGSC e-Procurement Solution Service Infrastructure.						
E2.254	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must protect the integrity and confidentiality of PWGSC e-Procurement Solution Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms (see subsection Encryption Standards) unless otherwise protected by alternative physical measures approved by PWGSC.						
E2.255	System and Communications Protection	The Contractor must a) create one or more Incident Tickets for each Incident detected by The Contractor or reported by PWGSC; and b) physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in PWGSC dedicated storage.						
E2.256	System and Communications Protection	Where layered safeguards are implemented (defence-in-depth solutions), the Contractor must implement solutions from different vendors at different layers within the network.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.257	System and Communications Protection	The PWGSC e-Procurement Solution Service Infrastructure must be physically and/or using virtualization technology, dedicated to PWGSC. The Contractor, at their discretion, can use non-dedicated hardware, non-dedicated software for the operation, administration and management of PWGSC e-Procurement Solution Service Management Data. Any use of non-dedicated hardware, non-dedicated software is only allowed for Email Solution Service Management Data according to the following conditions: a) must not access, process or store PWGSC e-Procurement Solution User Data; b) must not access, process or store PWGSC e-Procurement Solution System Data; c) must not access, process or store user account names and passwords; d) must be logically segregated from other client's data; e) must adhere to all PWGSC e-Procurement Solution Service Infrastructure requirements outlined in Annex 2 Security Requirements; f) must not access, process or store information labeled as Protected or Classified unless approved in writing by PWGSC; g) must not access, process or store service design information for the PWGSC e-Procurement Solution Service; and h) must not allow for the control or modification of the PWGSC dedicated PWGSC e-Procurement Solution Service Infrastructure.						
E2.258		The PWGSC e-Procurement Solution Service must include dedicated controls for any network interconnections between dedicated and non-dedicated PWGSC e-Procurement Solution Service Infrastructure, according to the approved Security Design, that includes:						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		a) boundary protection whereby, the Contractor must use current or previously evaluated physical firewall appliances (http://www.cse-cst.gc.ca/its-sti/services/cc/index-eng.html) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. The Contractor must obtain approval from PWGSC for alternative physical firewall appliances; b) integration of PWGSC provided threat detection equipment; c) incorporation of Contractor provided threat detection/prevention solutions; d) routing of traffic through authenticated proxy servers; and e) role based access control with least privilege.						
E2.259		The Contractor must a) physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in PWGSC dedicated storage; b) ensure that any network configuration details contained in any asset records and configuration records management systems for the PWGSC e-Procurement Solution Service Infrastructure are encrypted.; c) physically separate the network IP traffic of the PWGSC e-Procurement Solution System Data from all other PWGSC e-Procurement Solution Data; and d) logically separate the network IP traffic between the PWGSC e-Procurement Solution Service Management Data and the PWGSC e-Procurement Solution User Data.						
E2.260		The categorization of data for PWGSC e-Procurement Solution Services as either PWGSC e-Procurement Solution System Data, PWGSC e-Procurement Solution User Data or PWGSC e-Procurement Solution Service Management Data will be at the						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		sole discretion of PWGSC and based on comparison to other similar data.						
E2.261	System and Information Integrity	The Contractor must provide PWGSC with the e-Procurement Solution Service operational security procedures that includes operational roles and responsibilities for system and information integrity requirements specified in this SOW.						
E2.262	System and Information Integrity	The Contractor must define and execute the processes for patch management for the PWGSC e-Procurement Solution Infrastructure components that includes: a) ensuring the latest version of applications and operating systems are used; b) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; c) prioritizing critical patches using a risk-based approach; d) taking applications offline and bringing them back online; e) aligning criticality levels for patches as specified by PWGSC; f) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; and g) testing and verification methodology to ensure that patches have been implemented properly. h) defines the processes for patch management on custom software utilized within the PWGSC e-Procurement Solution Service Infrastructure that includes: i) identifying, reporting, and correcting flaws in custom software; ii) testing software updates related to flaw remediation for effectiveness and potential side effects on the Email Service before installation; iii) incorporating flaw remediation into the Email Service configuration management process;						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.263	System and Information Integrity	The Contractor must a) centrally manage the malicious code protection mechanisms; b) automatically updates malicious code protection/malware mechanisms (including signature definitions) within 6 hours of availability and as requested by PWGSC; c) prevents non-privileged users from circumventing malicious code protection capabilities; d) updates malicious code protection mechanisms only when directed by a privileged user; and e) does not allow users to introduce removable media into the PWGSC e-Procurement Solution Service Infrastructure.						
E2.264	System and Information Integrity	The Contractor must actively manage all network connections to external services associated with the PWGSC e-Procurement Solution Service Infrastructure as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by PWGSC; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and, and h) as necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies).						
E2.265	System and Information Integrity	The PWGSC e-Procurement Solution Service Infrastructure must provide near real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.266	System and Information Integrity	The PWGSC e-Procurement Solution Service Infrastructure must prevent all non-privileged users from circumventing intrusion detection and prevention capabilities.						
E2.267	System and Information Integrity	The PWGSC e-Procurement Solution Service Infrastructure **Security Event and Log Management Solution** must: a) include centralized and time-synchronised logging of allowed and blocked PWGSC e-Procurement Solution activity with regular log analysis; b) keep 3 months of events and logs online; c) keep events and logs associated with a security Incident for at least 2 years; d) store logs for at least 1 year; e) categorize events and logs based on Partners; and f) protect data and audit logs from unauthorized access, modification, and deletion.						
E2.268	System and Information Integrity	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by PWGSC, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by PWGSC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies PWGSC of the degree of non-compliance. In addition to any sources of intelligence on cyber threats and Incidents sources that the Contractor monitors in its routine operations, the Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.269	System and Information Integrity	The Contractor must implement a centrally managed Integrity Verification Solution to detect unauthorized changes to software and Email Infrastructure component configuration including: a) performing integrity scans at least every 30 days, and b) automatically generating a Security Incident Ticket upon discovering discrepancies during integrity verification.						
E2.270	System and Information Integrity	The PWGSC e-Procurement Solution Service Anti-Virus/Anti-Spam (AVS) Service must a) scan outbound and inbound messages for spam content in real-time; b) identify a message as spam based on a spam probability score (high, medium, low) specified by PWGSC; c) assign each spam classification as specified by PWGSC and an action to be taken if that threshold is exceeded; d) The Email AVS Service must respond to an Email Message identified as spam, as specified by PWGSC, that includes: a) discarding the Email Message (e.g. confirmed spam); b) tagging the subject field of the Email Message; c) sending the Email Message to a Mailbox and Email Folder specified by PWGSC (e.g. junk mail); d) replying to the Email Message with a bilingual warning message in the subject field, message body, and message header; and e) allowing the Email Message to be delivered based on content criteria specified by PWGSC (for example, words found in an Email subject line). c) Reject the message; d) Redirect the message; e) Quarantine the message; f) Modify the subject header of the message; g) support configuration of i) SPAM blacklists to allow customized entries as specified by						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		PWGSC; ii) SPAM whitelists to allow customized entries as specified by PWGSC; and iii) the sensitivity of the heuristic analysis as specified by PWGSC. h) make use of a Sender IP Reputation Service that shall accept or reject SMTP connections based on the reputation of the sender IP address, before the message is accepted for processing; i) The Sender IP Reputation Service shall include in its reputation verification hosts that are published in a public DNS Block List (DNSBL); j) If the reputation score for a sender IP address exceeds a configurable threshold, the Sender IP Reputation Service shall reject the sender's SMTP connections; and k) System events related to Sender IP reputation service will be logged and sent to Canada.						
E2.271	System and Information Integrity	The PWGSC e-Procurement Solution AVS Service must a) automatically update spam signature updates automatically at regular intervals to ensure that the SPAM signatures are always up to date and based on analysis of SPAM messages collected from various external SPAM databases by the Contractor; b) automatically update spam signatures and Spam Blacklists within 15 minutes of availability or at frequency specified by PWGSC; and c) apply security updates of signatures and Spam Blacklists within 15 minutes of receiving the updates.						
E2.272	System and Information Integrity	The PWGSC e-Procurement Solution Service, where assisted data entry is required in the input fields with pre-defined values are populated using lists, drop-down lists, checkboxes and radio buttons in plain language; a) assisted data entry where input fields with embedded meaning (i.e. multiple data elements concatenated within the same input field) are populated using a combination of lists, drop-down lists,						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		checkboxes and radio buttons in plain language for predefined values and textboxes for user provided values; b) error verification where input fields are verified for format and validity, including cross-field validation, with detailed error messages in plain language that indicate to the user what is incorrect and what is the rule(s) that failed; and c) pre-defined fields (e.g. service, work type, contact name, unit pricing, item number, quantities, etc.) approved by PWGSC, with assisted data entry (where applicable) to minimize error entries.						
E2.273	Data Security & Information Lifecycle Management Data Inventory / Flows	The PWGSC e-Procurement Solution Service policies and procedures must be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, Contractor must ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.						
E2.274	Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	The PWGSC e-Procurement Solution Service policies and procedures must be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance must be implemented for objects that act as aggregate containers for data.						
E2.275	Data Security & Information Lifecycle Management Non-Production Data	The PWGSC e-Procurement Solution Service production data must not be replicated or used in non-production environments.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.276	Data Security & Information Lifecycle Management Ownership / Stewardship	All PWGSC e-Procurement Solution Service data must be designated with stewardship, with assigned responsibilities defined, documented, and communicated.						
E2.277	Data Security & Information Lifecycle Management Secure Disposal	Any use of PWGSC e-Procurement Solution Service Production data in non-production environments requires explicit, documented approval from PWGSC whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.						
E2.278	Datacenter Security Asset Management	The PWGSC e-Procurement Solution Service assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time must be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.						
E2.279	Datacenter Security Controlled Access Points	The PWGSC e-Procurement Solution Service physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) must be implemented to safeguard sensitive data and information systems.						
E2.280	Datacenter Security Equipment Identification	The Contractor must ensure that automated equipment identification is used as a method of connection authentication for PWGSC e-Procurement Solution Service infrastructure as approved by the PWGSC to validate connection authentication integrity based on known equipment.						
E2.281	Datacenter Security	PWGSC authorization must be obtained prior to relocation or transfer of the PWGSC e-Procurement Solution Service hardware, software, or data to an offsite premises.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
	Off-Site Authorization							
E2.282	Datacenter Security Off-Site Equipment	The PWGSC e-Procurement Solution Service operational policies and procedures must be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This must include a wiping solution or destruction process that renders recovery of information impossible. The erasure must consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.						
E2.283	Datacenter Security Policy	The PWGSC e-Procurement Solution Service operational policies and procedures must be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.						
E2.284	Datacenter Security - Secure Area Authorization	The PWGSC e-Procurement Solution Service specific ingress and egress to secure areas must be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.						
E2.285	Datacenter Security Unauthorized Persons Entry	The PWGSC e-Procurement Solution Service specific ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises must be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.						
E2.286	Datacenter Security User Access	All physical access to the PWGSC e-Procurement Solution Service information assets and functions by users and support personnel must be restricted.						
E2.287	Encryption & Key	The PWGSC e-Procurement Solution Service PKI keys must have identifiable owners (binding keys to identities) and there must be key management policies.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
	Management Entitlement							
E2.288	Encryption & Key Management Key Generation	The PWGSC e-Procurement Solution Service operational policies and procedures must be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, Contractor must inform the PWGSC of changes within the cryptosystem, especially if the PWGSC e-Procurement Solution Service data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.						
E2.289	Encryption & Key Management Sensitive Data Protection	The PWGSC e-Procurement Solution Service operational policies and procedures must be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.						
E2.290	Encryption & Key Management Storage and Access	The PWGSC e-Procurement Solution Service platform and data-appropriate encryption (in compliance with CSE guidance ITSG-111) in open/validated formats and standard algorithms must be required. Keys must not be stored in the cloud (i.e. at the e-Procurement Solution Service cloud Contractor in question), but maintained by the PWGSC or trusted key management Contractor as mutually agreed upon with PWGSC. The PWGSC e-Procurement						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		Solution Service key management and key usage must be separated duties.						
E2.291	Governance and Risk Management Data Focus Risk Assessments	The PWGSC e-Procurement Solution Service risk assessments associated with data governance requirements must be conducted at planned intervals as mutually agreed upon with PWGSC and must consider the following: a) Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure; b) Compliance with defined retention periods and end-of-life disposal requirements; and c) Data classification and protection from unauthorized use, access, loss, destruction, and falsification.						
E2.292	Governance and Risk Management Management Oversight	The PWGSC e-Procurement Solution Service managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.						
E2.293	Governance and Risk Management Management Program	The PWGSC Contractor must have an Information Security Management Program (ISMP) developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program must include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: a) Risk management b) Security policy c) Organization of information security d) Asset management e) Human resources security f) Physical and environmental security						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		g) Communications and operations management h) Access control i) Information systems acquisition, development, and maintenance						
E2.294	Governance and Risk Management Management Support/Involvement	The PWGSC Contractor executive and line management must take formal action to support information security through clearly-documented direction and commitment, and must ensure the action has been assigned.						
E2.295	Governance and Risk Management Policy	The PWGSC Contractor information security policies and procedures must be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.						
E2.296	Governance and Risk Management Policy Impact on Risk Assessments	The PWGSC e-Procurement Solution Service risk assessment results must include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.						
E2.297	Governance and Risk Management Policy Reviews	The PWGSC Contractor's business leadership (or other accountable business role or function) must review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		applicability to legal, statutory, or regulatory compliance obligations.						
E2.298	Governance and Risk Management Risk Management Framework	All PWGSC e-Procurement Solution Service risks must be mitigated to an acceptable level. Acceptance levels based on risk criteria must be established and documented in accordance with reasonable resolution time frames and stakeholder approval.						
E2.299	Human Resources Asset Returns	The Contractor upon termination of workforce personnel and/or expiration of external business relationships, all PWGSC e-Procurement Solution Service-owned assets must be returned within an established period.						
E2.300	Human Resources Employment Termination	The Contractor roles and responsibilities for performing employment termination or change in employment procedures for PWGSC e-Procurement Solution Service must be assigned, documented, and communicated.						
E2.301	Human Resources Mobile Device Management	The Contractor must establish policies, procedures, supporting business processes, and implement technical measures, to manage business risks associated with permitting mobile device access to PWGSC e-Procurement Solution Service resources and must enforce the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring) as approved by PWGSC.						
E2.302	Human Resources Roles / Responsibilities	The Contractor must document the roles and responsibilities of contractors, employees, and third-party users as they relate to PWGSC e-Procurement Solution Service information assets and security.						
E2.303	Human Resources	Policies and procedures must be established, and supporting business processes and technical measures implemented, for						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
	Technology Acceptable Use	defining allowances and conditions for permitting usage of Contractor-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to Contractor's corporate resources (i.e., BYOD) must be considered and incorporated as appropriate.						
E2.304	Human Resources User Responsibility	All Contractor personnel must be made aware of their roles and responsibilities for: a) Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations; and b) Maintaining a safe and secure working environment						
E2.305	Human Resources Workspace	Policies and procedures must be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.						
E2.306	Infrastructure & Virtualization Security Clock Synchronization	The PWGSC Contractor must use a reliable and mutually agreed upon external time source to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.						
E2.307	Security Incident Management, E-Discovery & Cloud Forensics Incident Management	The PWGSC e-Procurement Solution Service must establish policies, procedures, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures approved by PWGSC.						
E2.308	Security Incident Management, E-	The PWGSC Contractor workforce personnel and external business relationships must be informed of their responsibilities and, if						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
	Discovery & Cloud Forensics Incident Reporting	required, must consent and/or contractually agree to report all information security events in a timely manner. Information security events must be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.						
E2.309	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Legal Preparation	The PWGSC Contractor must implement proper forensic procedures, including chain of custody, as required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, PWGSC and/or other external business partners impacted by a security breach must be given the opportunity to participate as is legally permissible in the forensic investigation.						
E2.310	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Metrics	The PWGSC Contractor must put in place mechanisms to monitor and quantify the types, volumes, and costs of information security incidents.						
E2.311	Supply Chain Management, Transparency and Accountability Data Quality and Integrity	The PWGSC Contractor must a) inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks; and b) design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.						
E2.312	Supply Chain Management, Transparency and Accountability	The PWGSC Contractor must make security incident information available to all affected customers, including PWGSC and Contractors periodically through electronic methods (e.g. portals).						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
	Incident Reporting							
E2.313	Supply Chain Management, Transparency and Accountability Contractor Internal Assessments	The PWGSC Contractor must perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.						
E2.314	Supply Chain Management, Transparency and Accountability Supply Chain Agreements	The PWGSC Contractor must incorporate at least the following mutually-agreed upon provisions and/or terms: a)Scope of business relationship and services offered (e.g., PWGSC (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of PWGSC Contractor and PWGSC (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) b) Information security requirements, PWGSC Contractor and PWGSC (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships c)Notification and/or pre-authorization of any changes controlled by the PWGSC Contractor with PWGSC (tenant) impacts d) Timely notification of a security incident (or confirmed breach) to all PWGSC (tenant) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		e) Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed f) Expiration of the business relationship and treatment of PWGSC (tenant) data impacted g) PWGSC (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence						
E2.315	Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	The PWGSC Contractor must review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.						
E2.316	Supply Chain Management, Transparency and Accountability Supply Chain Metrics	The PWGSC Contractor must a) implement Policies and procedures to ensure the consistent review of service agreements (e.g., SLAs) between contractor and PWGSC (tenant) across the relevant supply chain (upstream/downstream). b) Perform at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.317	Use of Zone Interface Point Firewall	The PWGSC e-Procurement Solution Service Design Boundary system in all Zone Interface Point (ZIP) must contain firewalls which perform state full packet inspection for infrastructure containing applications of **MEDIUM injury** and / or higher PWGSC Selections: - All PAZs, RZs, HRZs, SAZs, REZs - All zones of high and very high injury						
E2.318	Use of Zone Interface Point Firewall	The Contractor must ensure that all firewalls in all Zone Interface Point (ZIP) must be at minimum EAL4 certified (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.319	Use of Internal Boundary System Firewall	The Contractor must use firewalls which perform stateful packet inspection in internal boundary systems within all zone(s) for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.320	Use of Internal Boundary System Firewall	The Contractor must use physical firewall in internal boundary systems within a all zone(s) for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.321	Use of Internal Boundary System Firewall	The PWGSC e-Procurement Solution Service Infrastructure firewalls in all internal boundary systems must be at minimum EAL4 or common criteria certified (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.322	Use of Internal Boundary System Physical Devices	The PWGSC e-Procurement Solution Service Internal boundary systems in all zone(s) must contain physical or virtual devices for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.323	Zone Internetwork	The PWGSC e-Procurement Solution Service infrastructure use of virtual devices in the zone internetwork must be sufficiently						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
	Device Partitioning	partitioned from virtual servers in all zones for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.324	Use of Zone Internetworking Physical Devices	The Contractor must use physical and/or virtual devices as approved by PWGSC in the zone internetwork in all zones for infrastructure containing applications of PWGSC e-Procurement Solution Service.						
E2.325	Internetworking Traffic Partitioning	The PWGSC e-Procurement Solution Service Design specific virtual devices in the zone internetwork must not perform routing in Management and Restricted zones for infrastructure containing e-Procurement databases.						
E2.326	Storage Partitioning	PWGSC e-Procurement Solution Storage used by the hypervisor for virtual device images must be **physically and/or logically** partitioned for PWGSC e-Procurement Solution infrastructure containing applications of PROTECTED B with MEDIUM injury as defined by PWGSC.						
E2.327	Use of Hypervisor Features	The PWGSC e-Procurement Solution Service Design specific Virtual machines must not use any machine to machine sharing mechanism (e.g. file sharing) which is implemented within the hypervisor						
E2.328	Virtual Machine Distribution	The PWGSC e-Procurement Solution Service specific Virtual machines must be distributed via a **random, pseudo random or other** algorithm as approved by PWGSC.						
E2.329	Virtual Machine Distribution	The PWGSC e-Procurement Solution Service Design specific Virtual machines must be distributed such that there are **at least five (5) machines sharing** any physical resource for all physical resources.						
E2.330	Hypervisor Certification	The Contractor must use current or previously evaluated hypervisors managing all zones, as defined within the CSE ITSG-22 (https://cse-cst.gc.ca/en/node/268/html/15236) & ITSG-38 (https://cse-cst.gc.ca/en/node/266/html/25034) guidelines, (https://cse-cst.gc.ca/en/canadian-common-criteria-						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		scheme/main) validated under a recognized Common Criteria scheme against an approved Protection Profile that considers hypervisor evaluation for virtual machines protection between zones or obtain approval from PWGSC for alternative products						
E2.331	ICAM	The Contractor's Interim ICAM Solution must remove all credentials once fully migrated to Canada's GC ICAM solution.						
E2.332	Datacenter Security	The PWGSC e-Procurement Solution Service equipment and infrastructure must be housed by the Contractor in a suitable facility that is rated as Tier "II" Data Center at minimum by Uptime Institute "Tier Standard: Operational Sustainability" (https://uptimeinstitute.com/consulting-certification/operations/tier-certification-of-operational-sustainability) or equivalent, equipped with but not limited to the following features. a) Redundant high speed internet connectivity through multiple carriers; b) Redundant computer grade HVAC; c) Redundant UPS and Generators; d) Multi-homed internet backbone; e) 24/7 monitoring and server support; f) Firewall security and Intrusion detection; and g) Physical security measures to prohibit access by unauthorized parties.						
E2.333	Infrastructure & Virtualization Security Change Detection	The Contractor must ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.334	Infrastructure & Virtualization Security Management - Vulnerability Management	The Contractor must ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware) within the PWGSC e-Procurement Solution Service.						
E2.335	Infrastructure & Virtualization Security Network Security	The Contractor must ensure that the network environments and virtual instances must be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations must be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls as approved by PWGSC.						
E2.336	Infrastructure & Virtualization Security OS Hardening and Base Conrols	The Contractor must ensure that each operating system used within the PWGSC e-Procurement Solution Service is hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.						
E2.337	Infrastructure & Virtualization Security Production / Non-Production Environments	The PWGSC e-Procurement Solution Service production and non-production environments must be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		duties for personnel accessing these environments as part of their job duties as approved by PWGSC.						
E2.338	Infrastructure & Virtualization Security Segmentation	The Contractor's multi-tenant e-Procurement Solution Service-owned or managed (physical and virtual) applications, and infrastructure system and network components, must be designed, developed, deployed and configured such that provider and PWGSC (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: a) Established policies and procedures; b) Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance; and c) Compliance with legal, statutory and regulatory compliance obligations.						
E2.339	Infrastructure & Virtualization Security VM Security - vMotion Data Protection	The Contractor must use secured and encrypted communication channels when migrating physical servers, applications, or data to virtualized servers associated with PWGSC e-Procurement Solution Service and, where possible, must use a network segregated from production-level networks for such migrations.						
E2.340	Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	The Contractor must ensure that access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems for PWSGC e-Procurement Solution Service be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls,						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
		and TLS encapsulated communications to the administrative consoles).						
E2.341	Infrastructure & Virtualization Security Wireless Security	The Contractor PWGSC e-Procurement Solution Service policies and procedures must be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: a) Perimeter firewalls implemented and configured to restrict unauthorized traffic b) Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings); c) User access to wireless network devices restricted to authorized personnel; and d) The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network.						
E2.342	Infrastructure & Virtualization Security Network Architecture	The PWGSC e-Procurement Solution Service network architecture diagrams must clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures must be implemented as approved by PWGSC and must apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.						

EPS RFP Sec ID	Requirement Category	Security Requirement Statement	SOW Reference	Assessment Method	Assessment Criteria	Security Assessment & Authorization (SA&A) Gates		
						Gate 1 – Tracing to High Level Security Design Specification (How Addressed)	Gate 2 – Tracing to Detailed Level Security Design (How Addressed)	Gate 3 – Tracing to Integration Verification and Validation (How Addressed)
E2.343	Interoperability & Portability Virtualization	The Contractor must use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and must have documented custom changes made to any hypervisor in use and all PWGSC e-Procurement solution-specific virtualization hooks available for PWGSC review.						

ANNEX 3

PRICE SCHEDULE

Table of Contents

1. EPS Transition-In Fee

For the entirety of the Work described in Part 6, section 6.3 to 6.5 of the Statement of Work in Annex 1.	$_____ (Expressed as a Firm Lump Sum Fee in Canadian dollars, custom duties included, Applicable Taxes are extra)

Schedule of Milestones

Transition Phase	Milestone / Deliverable Title	Deliverable Date	Description	Percentage of Firm Lump Sum Fee Paid Upon Completion of Milestone
Planning and Mobilization	Detailed Implementation Plan	Within 45 days of Contract Award	Delivery of a Detailed Final Implementation Plan	2.5%
	Solution Environment	Within 90 days of Contract Award	The solution environments, as detailed in the SOW, are operational and ready for system configuration and testing	2.5%
Core Capability	Supplier Registration	Within 1 year of Contract Award	This milestone is reached when public registration of suppliers is opened and 1000 suppliers have registered	5%
	Contract Management	Within 1 year of Contract Award	This milestone is reached after the first 100 “live” contracts are awarded in EPS	10%
	Catalogues	Within 1 year of Contract Award	This milestone is reached after clients process 1000 “live” transactions through the EPS Catalogue	10%
Advanced Capability	Service Procurement	Within 2 years of Contract Award	This milestone is reached after 100 “live” SOW based service procurements are transacted through EPS	10%
	Vendor Performance	Within 2 years of Contract Award	This milestone is reached after 25 vendor performance surveys are conducted	5%

Transition Phase	Milestone / Deliverable Title	Deliverable Date	Description	Percentage of Firm Lump Sum Fee Paid Upon Completion of Milestone
	Government Electronic Tendering System (Critical Deliverable)	Within 2 years of Contract Award	This milestone is reached when EPS is official designated Canada's "Government Electronic Tendering System"	15%
Operations	AP On boarded (Critical Milestone)	Within 1.5 years of Contract Award	This milestone is reached when all procurement officers in the Acquisitions Program are managing contracts in EPS (legacy contract system no longer in use)	20%
	Fully Implemented (Critical Milestone)	Within 2.5 years of Contract Award	All EPS functionality, as detailed in the SOW, are operational within the production environment.	20%
Total				100%

2. EPS Operational Fee

2.1 Tier 1: 1 to 5,000 Users – Monthly Lump Sum Fee

For all authorized Work in accordance with all sections of the Statement of Work in Annex 1, with the exception of Part 6, section 6.3 to 6.5 and Part 7.	$_____ per month (Expressed as a Monthly Lump Sum Fee in Canadian dollars, custom duties included, Applicable Taxes are extra)

2.2 Tier 2: in excess of 5,000 Users – Monthly Ceiling Rate per User

For all authorized Work in accordance with all sections of the Statement of Work in Annex 1, with the exception of Part 6, section 6.3 to 6.5 and Part 7.	$_____ per User, per month (Expressed as a Firm Monthly Rate per User in Canadian dollars, custom duties included, Applicable Taxes are extra)

2.3 Tier 3: Unlimited Users – Monthly Lump Sum Fee

For all authorized Work in accordance with all sections of the Statement of Work in Annex 1,	$_____ per month

with the exception of Part 6, section 6.3 to 6.5 and Part 7.	(Expressed as a Monthly Lump Sum Fee in Canadian dollars, custom duties included, Applicable Taxes are extra)

3. Optional Services Fees – Task Authorizations

3.1 Optional Work

For the Work described in section *7.2.3 – Tender Feeds* of the Statement of Work in Annex 1.	$_____ (Expressed as a Fixed Price in Canadian dollars, custom duties included, Applicable Taxes are extra)
For the Work described in section *7.2.4 – Data Escrow* of the Statement of Work in Annex 1.	$_____ (Expressed as a Fixed Price in Canadian dollars, custom duties included, Applicable Taxes are extra)

3.2 Professional Services – Firm Per Diem Rates

Professional Service Category	Level	Per Diem Rate
A.1 Application/Software Architect	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
A.6 Programmer/Software Developer	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
A.8 System Analyst	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
A.12 WEB Architect	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
A.14 WEB Developer	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
I.1 Data Conversion Specialist	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
I.5 IM Architect	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
I.11 Technology Architect	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
B.1 Business Analyst	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
B.5 Business Process Re-engineering Consultant	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
B.7 Business Transformation Architect	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
P.1 Change Management Consultant	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
P.4 Organizational Development Consultant	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
C.3 IT Security TRA and C&A Analyst	Level 1	$_____
	Level 2	$_____
	Level 3	$_____

C.6 IT Security Engineer	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
C.7 IT Security Design Specialist	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
C.8 Network Security Analyst	Level 1	$_____
	Level 2	$_____
	Level 3	$_____
C.11 IT Security VA Specialist	Level 1	$_____
	Level 2	$_____
	Level 3	$_____

4. Annual Inflation Adjustment

The e-Procurement Solution Operational Fee and all Professional Services Per Diem Rates are subject to an annual inflation adjustment as of April 1, 2020. The adjustment will be equal to the increase in the all-items Consumer Price Index, monthly (CANSIM Table 326-0020) for January of that year over the same Index for the previous January**,** as published by Statistics Canada for the previous year. Any subsequent adjustments will be calculated on the most recent previous e-Procurement Solution Operational Fee and Professional Services Per Diem Rate. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

Inflation Adjustment – EXAMPLE

Had the annual inflation adjustment been applied in April of 2015, then the e-Procurement Solution Operational Fee for the subsequent annual period (April 1, 2015 - March 31, 2016) would have been adjusted as follows:

Annual Inflation Adjustment Rate would be:
= ((All-items CPI January 2015 / All-items CPI January 2014)-1)
= ((124.3 / 123.1) – 1)
= 0.0097
= 0.97%

e-Procurement Solution Operational Fee for 2015-16 would be:
= (e-Procurement Solution Operational Fee for 2014-15) X (1 + 0.0097)

ANNEX 4

SECURITY REQUIREMENTS CHECK LIST (SRCL) & SECURITY CLASSIFICATION GUIDE (SCG)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN578131350 REV #5
Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Public Works and Government Services Canada	Acquistions

3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work - Brève description du travail

e-Procurement Solutions Initiative

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No Non	☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No Non	☐ Yes Oui
6. Indicate the type of access required - Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non	☑ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p.ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No Non	☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciales sans entreposage de nuit?	☑ No Non	☐ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays : Please refer to Annex 1 - List of approved Countries by ISP	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :
☑ No / Non ☐ Yes / Oui

9. Will the supplier require access to extremely sensitive INFOSEC information or assets:
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?
☑ No / Non ☐ Yes / Oui

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET - SIGINT / TRÈS SECRET - SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : Refer to the attached security classification guide for details.

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
☐ No / Non ☑ Yes / Oui

If Yes, will unscreened personnel be escorted:
Dans l'affirmative, le personnel en question sera-t-il escorté?
☐ No / Non ☑ Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?
☐ No / Non ☑ Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?
☑ No / Non ☐ Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?
☑ No / Non ☐ Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?
☐ No / Non ☑ Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?
☑ No / Non ☐ Yes / Oui

PART C *(continued)* / PARTIE C *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	Confidential Confidentiel	Secret	Top Secret Très Secret	NATO Restricted NATO Diffusion Restreinte	NATO Confidential NATO Confidentiel	NATO Secret	COSMIC Top Secret COSMIC Très Secret	Protected Protégé A	 B	 C	Confidential Confidentiel	Secret	Top Secret Très Secret
Information / Assets Renseignements / Biens		✓														
Production																
IT Media Support TI		✓														
IT Link Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉ et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée.

12. b) Will the document attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN578131350 REV #5
Security Classification / Classification de sécurité
UNCLASSIFIED

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Franco, Emilio	Lead, Acquisitions Digital Program	

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date
(819) 956-1184	(819) 956-8303	emilio.franco@tpsgc-pwgsc.gc.ca	2015-03-05

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Forget, Rachelle	SO	

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date
(819) 956-0639	(819) 934-1449	rachelle.forget@tpsgc-pwgsc.gc.ca	17/11/2015

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?
☐ No / Non ☑ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date
(___) ___-____	(___) ___-____		

17. Contracting Security Authority / Autorisé contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date
(___) ___-____	(___) ___-____		

Terms and Definitions

Table 1 below summarizes the terms as used within this SCG and associated definitions.

Table 1: Definitions

Term	Definition
Administrator/ Privileged User	Person who manages user privileges and accounts of the **EPS**. This person can be a GC resource or **EPS** contractor resource.
Classification Level	An indicator or the sensitivity of the **EPS** information, i.e.: Protected A, Protected B, Unclassified, and other classifications specified by Government of Canada (GC).
Client	Any GC-owned or managed user agent or application that connects to the **EPS**.
Contractor	The person, entity or entities named in the Contract to supply goods, services or both to Canada
Contractor Facility	Means Data Center, SOC, Help Desk and any supporting service hosted within Contractor's facility
EPS Data	All data associated with **EPS**, including EPS User Data, **EPS** Operational Data, on any media.
EPS Operational Data	Any administration and management data generated by the **EPS** Infrastructure, on any media, such as security violations, transactions, audit records, alarm incident records, reports, logs, backups.
EPS Infrastructure	All hardware and software that processes and stores EPS Data and that Operators use to manage **EPS**.
External End Users	A Non-GC person that is authorized to use the **EPS**.
GC End Users	A GC resource (employee, contractor, etc.) that is authorized to use the **EPS**.
Host	Means any Internet Protocol (IP) addressable entity connected to an IP-based network.
Incident	Event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.

Table 1: Definitions

Term	Definition
Incident Management	Standardized methods and procedures to restore a service to normal operation as quickly as possible and to minimize the impact on business operations
Contractor Operations Centre	Contractor location that includes infrastructure and resources required for the centralized management and operation of the **EPS**. There are Two types of operations centers a. Network Operations Center (NOC), and b. Security Operations Center (SOC).
Operator	A Contractor resource which administers **EPS** Infrastructure.
Problem	Unknown cause of one or more Incidents often identified as a result of multiple similar Incidents.
Problem Management	Standardized methods and procedures to minimize the impact of Problems for **EPS**.
Public User	General population or community that is not an authorized user of the **EPS**.
Public/Open Data	Information that has no classification as it covers or details publicly available information.
Material Resource	A Room or Equipment.
SaaS	Software as a Service (SaaS) refers to the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Secure Perimeter	Logical and physical boundary around network accessible resources and information, which is controlled and protected against unauthorized access from outside of the boundary.

Table 1: Definitions

Term	Definition
Security Incident	An unauthorized behaviour (against the security policy of the IT system) regarding the operation and administration of the IT system that has the potential to compromise the IT systems confidentiality, integrity, or availability.
Managed Service	An electronic service configured, implemented, operated and managed by the service provider, including the supporting software, infrastructure, upgrades, maintenance and support.
Service Delivery Point (SDP)	Physical location in a building where the **EPS** is implemented.
Solution User Data	Includes Account, Notifications, Customized views and filters.
Supplier	Represents External users of the **EPS** that will be using the **EPS** to offer their services in response to various tenders published by GC.

Table 2 below outlines the personnel and facility security clearance requirements based on the expected roles, high-level EPS data access, and location of the data access.

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
1.	Public Users who will need to access 'Open/Public' information related to tenders being posted or contracts awarded by GC through the EPS.	• Public/Open Business Data; • Contract Award Notifications (CANs) in the EPS; • Very Limited Financial Information (Only the actual value of the Contract as identified in the CAN in the EPS).	Both (refer to information flow IF-A in Figure 3 below)	N/A	N/A	No	EPS Contractor	These are external public users browsing the EPS portal for public/UNLCASS information. EPS Contractor to ensure the availability of the EPS for access by public as per the terms of Service Level Agreement (SLA).	The Public/OPEN information is not designated and hence available to public to view.
2.	External End Users including the supplier delegates who will need to access the information specific to their business and bid responses including company proprietary information.	• Business Data; • User credentials (each supplier has ownership of the assigned unique users accounts); • RFP submissions and associated supplier propriety information; • Supplier's financial information	Both (refer to information flow IF-A, IF-D, IF-E in Figure 3 below)	N/A[1]	N/A	No	EPS Contractor	These are external users of the EPS representing the supplier community.	These EPS end users will be processing, accessing and handling information specific to their company including pricing and proposal information in response to the GC tenders.

[1] Information local to supplier is under supplier's control and not GC responsibility. Once it is handed over to GC, information is deemed as Protected 'B'.

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
3.	Any EPS Contractor personnel with physical access to the EPS infrastructure at Contract Service Delivery Points (SDP), includes Contractor data centers, Security Operations Center (SOC), Network Operations Center (NOC). Additionally, physical segregation requirements will be separately identified within the EPS Contract.	• Physical hardware; • Service Delivery Point (Data Center Contractor / SSC); • Data as stored on the Contractor's local Backup Media	Canada (refer to information flow IF-C in Figure 3 below)	Protected 'B'	Secret[2]	Yes	EPS Contractor	This is for any Contractor personnel including facilities management resources that have physical access to the EPS hardware equipment at the Contractor SDP for SOC/NOC capabilities that will be separate from SSC SOC/NOC.	SSC SOC is dedicated for SSC internal services and associated resources. SSC most likely will not allow 3rd party resources to be collocated in SSC SOC facilities. The EPS deployment model will involve use of SSC Data Center facilities. The access to these facilities and infrastructure elements will be considered privileged access requiring the designated level of clearance.

[2] The SaaS Cloud deployment model that is hosted at Contractor's Data Center facilities will need to be cleared to FSC level as per the SRCL fro EPS.

									Following is extracted from TBS Policy 'Standard on Security Screening (refer to http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115&section=text for more details as listed in Appendix B section 2)' • Regular access to information, IT systems, and assets categorized as Protected A or B , Confidential and Secret • Unescorted access to reception, operations, and security zones of certain federal government facilities • Access to systems in security zones with

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
									permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up and recovery, testing, installation and configuration changes Any EPS Contractor Personnel with physical access includes the following categories of resources. • EPS dedicated Operations Support resources with administrative access to

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
									the EPS infrastructure and information; • EPS Security and Incident Management resources with privileged access to EPS infrastructure and information; • General purpose facilities maintenance staff as these resources will be performing physical maintenance and cleaning type activities at the Contractor SDP.
4.	Contractor Personnel during High Level Design (HLD) Phase	• Design Blueprint;	Both	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	Typically Subject Matter Expert's from outside of	

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
		• COTS products configuration details; • Hardware details; • Security policy and rules as applicable to EPS including perimeter controls and auditing	(Information Flow not applicable here)					Canadian Operations are likely to be pooled into the development of High Level Design. It is very likely that the expertise to provide guidance for enterprise level deployment as required to support EPS exists outside of Canada within the Contractor organization.	
5.	Contractor Key Resources providing services on the solution development and delivery team for the EPS	• Design Blueprint; • COTS products configuration details; • Hardware details; • Security policy and rules as applicable to EPS including perimeter controls and auditing	Both (Information Flow not applicable)	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	Only applicable to the Contractor's key resources providing the services identified in the role/function column.	These Contractor Key Resources are part of the solution development and delivery team for the EPS. These resources will have privileged access into the entire solution design. Of this information is disclosed in an unauthorized manner, adversaries will exploit it to initiate cyber-

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
									attacks on the EPS and supporting infrastructure.
6.	Contractor Application Integration Support as required through the design and development phases of the EPS	• Design Blueprint; • COTS products configuration details; • Hardware details; • Security policy and rules as applicable to EPS including perimeter controls and auditing	Both (Information Flow not applicable here)	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	These Contractor Resources are responsible for developing, installing and operating the components required for the integration of the EPS at the application layer with other GC Applications and/or Non-GC Applications. The nature of these activities will imply that these users have privileged access to be able to develop, implement and monitor the integrated components. These resources will have the intimate knowledge for the security configurations for various components at the application integration layer.	Any unauthorized access through this trusted back door function might render the entire EPS susceptible to exploits by adversaries.
7.	Contractor Security Operations Center(SOC) Personnel	• All Business Data; • Security Data including audit logs;	Canada (refer to information flow	Protected 'B'	Secret	Yes	EPS Contractor	All SOC personnel will have privileged access to EPS infrastructure and	SSC SOC is dedicated for SSC internal services

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
		• System configuration including security components; • Physical hardware; • Service Delivery Point (Data Center Contractor / SSC); • Backup Media	IF-C in Figure 3 below)					sensitive security incident data. Contractor SOC personnel will need privilege access to be able to monitor and react to remediate any problems that threaten the security and/or availability of the EPS. Additionally, these resources will have intimate knowledge of the security configurations for various components, including security components, within the EPS.	and associated resources. SSC most likely will not allow 3rd party resources to be collocated in SSC SOC facilities. Given the privileged access to IT/IS resources from within SOC infrastructure, any unauthorized access through this trusted back door function might render the entire EPS susceptible to exploits by adversaries.

									Following is extracted from TBS Policy 'Standard on Security Screening (refer to http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115&section=text for more details as listed in Appendix B section 2)' • Regular access to information, IT systems, and assets categorized as Protected A or B , Confidential and Secret • Unescorted access to reception, operations, and security zones of certain federal government facilities Access to systems in security zones

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
									with permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up and recovery, testing, installation and configuration changes
8.	Contractor Operations Center Personnel	• All Business Data; • Security Data including audit logs; • System configuration including security components; • Physical hardware; • Service Delivery Point (Data Center Contractor / SSC); • Backup Media	Canada (refer to information flow IF-C in Figure 3 below)	Protected 'B'	Secret	Yes	EPS Contractor	This is for Contractor personnel with privileged access including second and third level support. Contractor Operations personnel typically include system administrators, DBAs and this category of users will need privilege access to be able to monitor and react to remediate any problem that threaten the security and/or availability of the EPS. Additionally, these resources will have intimate knowledge of the security configurations for various	SSC SOC is dedicated for SSC internal services and associated resources. SSC most likely will not allow 3rd party resources to be collocated in SSC SOC facilities. Any unauthorized access through this trusted back door function might render the entire EPS susceptible to exploits by adversaries.

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
								components, including security components, within the EPS.	Following is extracted from TBS Policy 'Standard on Security Screening (refer to http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115&section=text for more details as listed in Appendix B section 2)' • Regular access to information, IT systems, and assets categorized as Protected A or B , Confidential and Secret • Unescorted access to reception, operations, and security zones of

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
									certain federal government facilities • Access to systems in security zones with permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up and recovery, testing, installation and configuration changes
9.	Contractor Service Desk Personnel	• All Business Data including RFP response for incident trouble shooting; • Security Data including login credential;	Both (refer to information flow IF-C in Figure 3 below)	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	These Contractor resources will be contacted by the end users	The Contractor's Service Desk Personnel will be the first line of support for both GC and non GC users. The activities related to

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
		• System configuration including security components; • Reporting; • Service Delivery Point (Data Center Contractor); • Incident ticketing system							troubleshooting an end user issue will likely expose them to sensitive information. In order to prevent any unauthorized disclosure of sensitive information through this channel, the security requirement is elevated compared to normal help desk function.
10.	Contractor's 4th Level Original Equipment Manufacturer (OEM) Support Personnel	• Business Data; • Security Data including login credential; • System configuration including security components; • Service Delivery Point (Data Center Contractor);	Both (refer to information flow IF-C in Figure 3 below)	Protected 'B'	N/A	No	EPS Contractor	The Contractor must get ACQB Project Authority approval prior to providing any EPS data/information to 4th level OEM Support for the purposes of troubleshooting. At any time during the operational life of the EPS, the 4th Level OEM resources will not have direct access to EPS or	As detailed these will be non GC and Non Contractor resources that will work under the operational guidelines established by Contractor and approved by ACQB for the OEM based

Table 2: EPS User Roles vs. Clearance Requirements

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada/Foreign /Both)	Expected Data Sensitivity Classification Level	Clearance Level	Reliability Screening	ACQB/Contractor Responsibility	Details	Rationale
		• Incident ticketing system						data/information stored within. The 4th Level OEM support personnel will be at the Contractor Service Delivery Points and will be escorted by cleared Contractor Operators at all time during their stay within the Service Delivery Points.	functions (typically referred to as local maintenance).

ANNEX 5

GLOSSARY

1.0 GLOSSARY OF TERMS

This section outlines key terms that are employed throughout the Statement of Work (SOW). This annex should be used in conjunction with Annex 6 - Acronyms.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A

Aboriginal Business: A business that is at least 51% Aboriginal owned and controlled; and, if the business has 6 or more full-time staff, at least one-third of them are Aboriginal people.

Acceptance Test Plan: Means the document which describes the tests that the Contractor must perform on the Work before submitting it to PWGSC for acceptance or delivery to PWGSC.

Access Control: Security Controls that support the ability to permit or deny access to resources within the information system.

Access right(s): A set of business rules and/or an approach to control, regulate or restrict system access to an authorized user according to his/her assigned role(s) and rights.

Active Clauses: Clauses that are not designated as expired and is at the given point can be used in the Solution.

Activity: An activity represents an operation on a business class or item that results in a change in the state of the business class or item. Activities are often modeled and represented in a workflow or activity diagram.

Actor: A user, system, solution or service that performs one or many business or system functions. An actor may represent a role played by a human user or a set of automated tasks completed by an external IT system.

Actual uptime: The actual time a service is operational without disruption.

Ad-hoc Analysis: Is the term commonly used in businesses to describe a product (analytical report, statistical analysis or model, or other report or summary of data) produced one time to answer a single, specific business question. The user can specify what type of report to create by having the ability to choose what data elements will be included, being able to specify how to group the data, and being able to choose from different output or format styles for the desired report.

Ad-hoc Approver: Is a role assigned, on a case by case basis, to define an additional level of approval throughout the procurement process.

Ad-Hoc Query: The ability to create a one-off, "on demand" report that addresses a specific business question.

Administrator: Is a role defined for managing advanced system functionalities.

Advanced search: An Advanced search offers more than one search field, and the user can narrow the search, both by searching based on more than one field at a time and by using a variety of search operators, such as starts with, contains, greater than, less than, Boolean, ranges (Dates, Numbers) on one or more of available fields, including free text.

Advanced Contract Award Notice (ACAN): A notice posted on the Government Electronic Tendering Service (GETS) advising suppliers in advance that a contract will be awarded to a particular supplier and to invite them to submit a statement of capabilities if they think that they meet the requirements set out in the ACAN**.**

Agency: Refer to Government entity definition in this annex.

Agent: Person who acts on behalf of another person (the principal) in dealings with third parties.

Analytics: Analytics is the application of mathematical formulas, statistics, queries, info cubes and other data objects to analyze various aspects of the e-Procurement Solution (EPS) such as buying habits; the classification of suppliers, products and services; volumetric; supplier value; sources of supply; and top supplier metrics.

Anonymity: The severing of sensitive information and their detailed records to prevent the discovery and ensure privacy and confidentiality.

Application Availability: The percentage of time the application (EPS) is available for normal business operations.

Application Programming Interface (API): An API is a set of routines, protocols, and tools for building applications, including interfaces that allow software and hardware components to communicate with each other.

Assets: Anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value is considered an asset.

Audit: A formal inspection to verify that standards and regulations are being followed, records are up-to-date and accurate, and/or business targets are being met. Refer to Compliance definition in this annex.

Authentication: Process to verify the digital identity of the sender of a network communication.

Authority: The right to perform certain acts, or prescribe rules governing the conduct of others. Under a balanced scheme of management, administrative authority represents the activation of corporate policy and it is coupled with responsibility and accountability. An authority may also be a person who is commonly regarded as possessing an extensive knowledge in any given field.

Back to TOP

B

Basket of Goods: Is a segmented portion of a larger grouping of products or services. Comparing bidder proposals on the basket of items allows the buying organization to award the entire portfolio of products/services to the best bidder.

Benchmark: A benchmark is a management method to compare the performance of like products or services.

Bid: An offer to provide services or supply goods as a result of a solicitation

Bidder: Person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both. It does not include the parent, subsidiaries or other affiliates of the bidder, or its subcontractors.

Bidding Transparency: A method of procurement that promotes suppliers' access to, and transparency in, the procurement process and facilitates Canada's receipt of best value.

Bid Solicitation: An invitation, to suppliers to submit a bid, quotation or offer.

Boolean Catalogue search: Allows you to combine words and phrases using the words AND, OR, NOT (known as Boolean operators) to limit, broaden, or define your search

Business day: Is any working day, Monday to Friday inclusive, excluding statutory and other holidays, and any other day which the Licensee has elected to be closed for business.

Business Intelligence (BI): BI is the set of techniques and tools for the transformation of raw data into meaningful and useful information for business analysis purposes. The goal of BI is to allow for the easy interpretation of large volumes of data and identifying new opportunities and implementing an effective strategy to evaluate new opportunities.

Business Number: A unique, nine-digit business number that is given to your registered business by the Canada Revenue Agency as an identifier.

Business requirement: A precise statement that describes a specific characteristic or element of a business, product, solution or service to address a defined business need. A business requirement outlines a business objective that will solve a problem, meet a standard or provide a requisite business function.

Business rule: A specific, practicable, testable directive that is under the control of the business and that serves as a criterion for guiding behaviour, shaping judgments, or making decisions.

Buyer: A purchasing agent within an organization. Buyers can include Procurement/Contracting Officers from governments (including their respective ministries, departments, crown corporations and agencies), other publicly-funded organizations who must follow open procurement policies and are subject to various trade agreements.

Back to TOP

C

Call Abandonment Rate: Parameter to measure the percentage of all inbound Service Desk calls in the queue (i.e., calls where the caller has completed menu selection and is waiting in queue for a Service Desk agent) in which the caller hangs up before the EPS Service Provider's Service Desk agent answers the call.

Catalogue: An organised descriptive list of products or services made available by suppliers to potential buyers via the Internet. This allows contracting authorities to manage their catalogues online, to share their catalogues with other authorities and to handle orders electronically. Suppliers can upload their catalogue, submit it for approval through the application and can receive orders electronically.

Ceiling Price: The maximum price to be paid to the contractor as established in the contract and beyond for which the contractor will not receive additional compensation for the defined work.

Central Repository: The central repository serves as the central hub for all associated repositories. Refer to clause repository, supplier repository, and contract repository definitions in this annex**.**

Certificate Revocation List (CRL): As part of a Public-Key Infrastructure (PKI), CRLs specify the unique serial numbers of all revoked certificates. Prior to using a certificate, the client-side application must check the appropriate CRL to determine if the certificate is still trustworthy.

Change Management: Standardized methods and procedures used for efficient and prompt handling of all changes to PWGSC EPS Services, in order to minimize the number and impact of any related Incidents upon a Service.

Change Order: A method of modifying an existing purchase order or contract

Clause repository: A library of contract clauses that enable the central management and auto-generation of re-usable, standardized and custom terms, and contractual language. Refer to Contract repository and Supplier repository definitions in this annex.

Classification Level: An indicator or the sensitivity of the EPS information, i.e.: Protected A, Protected B, Unclassified, and other classifications specified by Government of Canada (GC).

Client: A public sector department, agency, branch, division, Crown Corporation or other entity for whom PWGSC procures goods and services.

Collaboration: The process whereby multiple internal and/or external parties work cooperatively to contribute ideas, information and previous experience for a specific purpose.

Closing Date: The date on which all submissions must be received by public notices.

Closing Time: Indicates the exact time and time zone which the submissions must be received by.

Commodity: Is any service or good such as, raw material, perishable goods, fabricated article or item of production or supply utilized in everyday endeavors and which is identified by contents, physical nature or characteristics.

Comparative Evaluation: A comparison of supplier quotes/bids for goods/services based on criteria such as: price, quantity, level of effort, lead time, and delivery performance to select a supplier.

Compliance: Verification that policies, practices, standards, regulations, guidelines and mandatory terms and conditions defined in a contract are being followed. Refer to Audit definition in this annex.

Comprehensive Land Claims Agreements (CLCAs):

1) Comprehensive Land Claims Agreements (CLCAs) are negotiated in areas of Canada where Aboriginal rights and title have not been addressed by treaty or through other legal means. These agreements are modern-day treaties between Aboriginal claimant groups, Canada and the relevant province or territory. While each one is unique, these agreements usually include such things as land ownership, money, wildlife harvesting rights, participation in land, resource, water, wildlife and environmental management as well as measures to promote economic development and protect Aboriginal culture. Many agreements also include provisions relating to Aboriginal self-government.

2) CLCAs are law, and take precedence over all trade agreements. The CLCA obligations are legally binding because they are contained in agreements signed by Canada and enforced by legislation.

Configurable: Settings that can be made, out-of-the-box without having to customize, to meet the GC services standards and requirements including IT architecture, functional, performance, availability, maintainability, security and Business Continuity/Disaster Recovery.

Configuration: Settings that can be made, out-of-the-box without having to write new code, to meet the GC services requirements including IT architecture, functional, performance, availability, maintainability, security and Business Continuity/Disaster Recovery.

Consumer-Like: Providing a business to consumer experience.

Contract Award Notice (CAN): Information on who has been awarded the contract.

Contract Operations Center: Contractor location that includes infrastructure and resources required for the centralized management and operation of the EPS. There are two types of operations centers Network Operations Center (NOC), and Security Operations Center (SOC).

Contracting Authority: The person authorized to enter into a contract on behalf of Canada.

Contracting Officer: Refer to Buyer in this annex.

Contract Lifecycle Management (CLM): The process of systematically and efficiently managing Contract creation, execution and analysis to maximize operational and financial performance and minimize risk. Refer to Contract management in this annex.

Contract management (or administration): A service that encompasses the management of a contract, contract amendment or agreement between GC and one or more suppliers. Contract management includes authoring, workflow, administration, amendment and storage of a contract or agreement throughout its lifecycle.

Contract repository: A repository that facilitates the flow (i.e., automatic aggregation, storage, retrieval, processing, routing and distribution) and control of contract documents and specific information linked to a procurement file in a secure, self-service environment. Refer to Clause repository and Supplier repository definitions in this annex.

Contractor: The person, entity or entities named in the Contract to supply goods, services or both to Canada.

Contractor Facility: A Data Center, Security Operations Center (SOC), Help Desk and any supporting service hosted within a Contractor's facility.

Controlled goods: Controlled goods are defined under the schedule to the Defence Production Act. The goods listed in the schedule to the Export Control List made under section 3 of the Export and Import Permits Act are controlled goods

Cost Centre (CC): An administrative unit selected within an organization for the purpose of accumulating and controlling costs.

Cross-PunchOut: Is part of a Catalogue Management system that connects a buyer to more than one supplier external web site from within the EPS. Refer to PunchOut in this annex.

Crown Corporation: Refer to Government entity definition in this annex.

Cutover: The switchover from an old system (hardware and/or software) to a new one. Cutover is the point at which a new system becomes operational.

Back to TOP

D

Data Architecture: Is composed of models, policies, rules or standards that govern which data is collected, and how it is stored, arranged, integrated, and put to use in data systems and in organizations.

Dashboard: An easy-to-read, real-time interface that displays the current status (snapshot) of specific information.

Data Center: A facility used to house computer systems and associated components, such as telecommunications and storage systems.

Data model: A data model organizes data_elements (qualitative or quantitative) and standardizes how the data elements relate to one another. A data model explicitly determines the structure of data.

Data warehouse : Is a system used for reporting and data analysis. DWs are central repositories of integrated data from one or more disparate sources. They store current and historical data and are used for creating analytical reports for knowledge workers throughout the enterprise.

Data visualization : A method of putting data in a visual or a pictorial context as a way to assist users in better understanding what the data are telling them (e.g., a map is a way to visualize which areas of the country get the most rainfall).

Database: Is an organized collection of data. It is the collection of schemes, tables, queries, reports, views and other objects.

Defect: A lack, want, deficiency or absence of something necessary for completeness, perfection or adequacy in form or function. An imperfection, fault or error in manufactured materiel and service.

Defence Supplies: Include only those specified goods that are, or may be, used directly or indirectly in the defence of Canada.

Delegate: Any person who is granted authorization to act on behalf of another individual to perform or approve a defined set of tasks.

Denial of Service: An attempt to make a machine or network resource unavailable to its intended users. Examples include: bandwidth attack, distributed denial of service, backscatter, consumption of system resource attack, communication obstruction, disruption of state information, disruption to routing/DNS information and web defacement.

Department: Refer to Government entity in this annex.

Departmental Financial and Material Management System (DFMS): The financial management system(s) used by a government entity; made up of instances using SAP, Oracle, Freebalance, CDFS, GX, and Peoplesoft.

Design Specification: Are the activities and deliverables associated with translating user and information system requirements into detailed technical specifications.

Digital Signature: The cryptographic transformation, which when added to a message, transaction, or record, allows the recipient to verify the signer and whether the initial information has been altered or the signature forged since the transformation was made.

Disposal: The removal of materiel from a supply system by sale, trade-in or destruction. Within the federal government, disposal is normally arranged through the PWGSC Crown Assets Distribution Directorate/Centre.

Disposition: A range of processes associated with implementing retention, destruction or transfer decisions which are documented in disposition or other instruments.

Document: A piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record.

Document Management: Is the coordination and control of the flow (storage, retrieval, processing, printing, routing, and distribution) of electronic and paper documents in a secure and efficient manner, to ensure that they are accessible to authorized personnel as and when required.

Dynamic Process Map: Allows user to customize and create on-demand processes for different scenarios rather than using default process map. Dynamic maps provide the flexibility to route requests to different locations dynamically. Refer to process map definitions in this annex.

Back to TOP

E

e-Auction: Is an online function between auctioneers and bidders, which takes place on an electronic marketplace. Refer to Reverse e-Auction in this annex

e-Learning Technologies: products that includes stand-alone, self-directed eLearning products to integrated, blended and hybrid approaches that combine a variety of delivery methods, tools, learning events and learning models.

Electronic Record: A record on electronic storage media, produced, communicated, maintained and/or accessed by means of electronic equipment.

Electronic signature: A signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document.

Electronic Bidding (e-Bidding): The ability to solicit electronic bids from suppliers.

Email Response Time: Parameter to measure the time for the EPS Service Provider to respond to e-mails received at the Service Desk. Time is measured from the time the e-mail is received to the time the e-mail is responded to and the EPS Service Provider's response is logged in the System.

End-User: Is a person who is authorized to use the solution. Refer to GC User, and External User in this annex.

Enterprise Service Bus (ESB): A software architecture model used for designing and implementing communication between mutually interacting software applications in a service-oriented architecture (SOA).

EPS Data: All data associated with EPS, including EPS User Data, EPS Operational Data.

EPS Infrastructure: All hardware, systems software, and facilities that process and manage the EPS.

e-Sourcing: A function that uses secure, web-based, collaborative tools to conduct strategic activities in the procurement lifecycle online, including identifying suitable suppliers, requirements definition, tendering, negotiation, Contract award and Contract management.

Estimated Cost: The estimated cost to be used as the basis for the sourcing decision is that cost determined, through consultation between PWGSC and the client, as being representative of all known work and expected unscheduled work, arising out of the requirement, that is, the total estimated contract value.

Exception Requests: Exception Requests relate to the activities associated with fulfilling End User requests for products or Services that are outside GC's standard policies.

Back to TOP

F

Fact Table: A fact table captures the data that measures the organization's business operations. Fact tables usually contain large numbers of rows, sometimes in the hundreds of millions of records when they

contain one or more years of history for a large organization. A key characteristic of a fact table is that it contains numerical data (facts) that can be summarized to provide information about the history of the operation of the organization.

Faceted search: A technique for accessing information organized according to a faceted classification system, allowing a User to explore a collection of information by applying multiple filters.

Filter: A mechanism that includes or excludes specific data from reports based on the user decision

First Contact Call Back: Parameter to measure the percentage of User contacts to the Service Desk (by telephone, e-mail, or other methods) which require the User to contact the Service Desk again (i.e., Call Back) regarding the same Service Request or Incident due to an insufficient or unsatisfactory resolution.

First Contact Resolution: Parameter to measure the percentage of User contacts to the Service Desk (by telephone, e-mail, or other methods) which are resolved by the Service Desk agent during the first contact.

First Point of Contact: First Point of Contact (FPOC) provides toll-free support for logging, tracking, resolution and reporting of Service Desk Incidents and Service Requests for all GC-supported environments.

Fixed time rate: A method of pricing in which the amount payable is determined in accordance with the combined cost of labour, overhead and profit, as expressed by a fixed amount by time period.

Fixed unit price: A method of pricing in which the total amount payable is the product of the number of identical units of work performed or identical items delivered, multiplied by a predetermined fixed price for each unit or item.

Floor Price: The minimum price that can be paid for a good or service as established in the contract.

Framework agreement: A general term for an agreement, or other arrangement, with a supplier(s), that establish terms and conditions under which specific purchases can be made throughout the term of the agreement. Referred to by Canada as: standing offers, supply arrangements, and contracts with task authorizations.

Functional requirement: A functional requirement defines a function of a system and its components. A function is described as a set of inputs, the behavior, and outputs.

Fuzzy Logic Search: Text retrieval technique based on finding matches even when keywords are misspelled or only hint of a concept.

Back to TOP

G

Government of Canada (GC) User: Is someone inside GC or other public organization who has access to private, internal knowledge and content within EPS and can use this knowledge to make decisions about the business.

Go-live date: The date the service will be implemented in production.

Goods or service: Are offered by a supplier for a defined market. Refer to commodity in this annex.

Goods and Services Identification Number (GSIN): A system of material and services categorization used within PWGSC. The system is used in conjunction with the Federal Supply Classification (FSC) code.

Government Electronic Tendering Service (GETS): The service used by the federal government to post notices (for example, Notices of Proposed Procurement, Advance Contract Award Notices and Contract Award Notices) and to make available solicitation documents.

Green Procurement: A policy designed to ensure that the government cost effectively procures, operates and disposes of its assets in a manner that protects the environment and supports sustainable development objectives.

Back to TOP

H

Historical Clauses: Clauses that are non-active and is at the given point in time not being used in the Solution.

Historical data: Past-periods data, used usually as a basis for forecasting the future data or trends. Data that may contain a significant fact, as of a certain point in time (e.g., a point-in-time report, database snapshot and version information).

Holdback: This refers to an amount withheld under a contract, to ensure the performance of the contract, and also to avoid overpayments in relation to progress of work.

Host: Means any Internet Protocol (IP) addressable entity connected to an IP-based network.

Back to TOP

I

Identity Credential and Access management (ICAM): A PWGSC EPS Service, owned and managed by the Contractor at their locations that can be ordered by PWGSC to provide credential management and authentication services and management of EPS Accounts

Incident: Is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

Incident Closure Notice: Parameter to measure the time by which the Service Desk provides a closure notice to a User who raised an Incident or made a Service Request to the Service Desk. Time is measured from the logging of Resolution of the Incident or completion of the Service Request in the System to the time of providing the closure notice to the User.

Incident Management: Is a process for logging, recording and resolving incident(s). The aim of incident management is to restore the service to the customer as quickly as possible rather than through trying to find a permanent solution.

Incident Resolution Escalation: Parameter to measure the elapsed time for Incidents received at the Service Desk to be escalated when it is determined that Incident Resolution requires Level X support. Measurement begins upon receipt of the Incident by the Service Desk and determination that it needs to be forwarded to Level X support, and ends at the time the Incident is forwarded to Level X support.

Infrastructure as a Service (Iaas): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).

Integration: is the process of bringing together the component subsystems into one system and ensuring that the subsystems function together as a system

Intelligent Requisition: Web-based requisition which can be configured with a business rules and business logic and respond appropriately to user's input. It streamlines ordering process and allows buyers to make intelligent product purchases. Intelligent requisition also makes it possible for users to link the clean, robust data into the existing requisition. It provides a simple, familiar ordering and online shopping experience.

Internal User: Refer to Government of Canada User in this annex.

Interoperability: Is a property or capability of a system or solution, whose interfaces are completely understood such that it works with other systems or solutions without any restricted access or implementation.

Intuitive: A desirable characteristic associated with the concept of usability. Within the context of EPS and the user interfaces with the service, intuitive means quick and ready insight by the user. It means that the process and specific tasks being executed are readily understood by the user without additional intervention of other guidance, information, or deductive reasoning.

Installation: Means the general installation services provided by the Contractor. The Installation services requirements are described in PWGSC EPS Annex A: SOW General subsection Installation and elsewhere in the Contract.

Inventory: This refers to an itemized list of goods or services, showing the number and usually the value of the items.

Invoice: A billing document prepared by the seller setting out the details of goods sold or services rendered to the purchaser.

Invitation To Tender (ITT): A bid solicitation document used by PWGSC when the estimated value of the requirement exceeds $25,000; two or more sources are considered capable of supplying the requirement; the requirement is adequately defined in all respects to permit the evaluation of tenders against clearly stated criteria; tenders can be submitted on a common pricing basis; and it is intended to accept the lowest-priced responsive tender without negotiations.

Back to TOP

J-K

Joint venture: Association of two or more parties who combine their money, property, knowledge, expertise or other resources in a single joint business enterprise, sometimes referred as a consortium, to bid together on a requirement

Jurisdictions: is an area with a set of laws under the control of a system of courts or government entity which are different from neighbouring areas. Canada is a federation with 11 distinct jurisdictions of governmental authority: the country-wide federal Crown and the 10 provincial Crowns. All are generally independent of one another in their respective areas of legislative authority

Key Performance Indicator (KPI): A type of performance measurement used to measure the success of a particular activity.

Knowledge base: A repository for performing knowledge management that provides the means to collect, organize, retrieve and share current or historical information (e.g., corporate knowledge). A knowledge-

based system uses artificial intelligence tools and may focus on a specific domain (e.g., procurement) to provide the insight, rationale and/or justification for making an informed decision. Knowledge is acquired and represented using various techniques, rules, frames and scripts.

Knowledge Management: Is the systematic management of an organization's knowledge assets for the purpose of creating value and meeting tactical & strategic requirements; it consists of the initiatives, processes, strategies, and systems that sustain and enhance the storage, assessment, sharing, refinement, and creation of knowledge.

Back to TOP

L-M

Letter of intent: A commitment to award a contract to a designated contractor. It may be used to authorize commencement of the work before the award of a contract, in those cases where the contract provisions require time-consuming negotiations, and the timely delivery of goods or services would be jeopardized by waiting for the award of the contract. A letter of intent is issued subsequent to approval of those terms and conditions, which have been already agreed to between Canada and the contractor, but before obtaining approval of all the terms and conditions of the proposed contract.

License Agreement: A contract by which permission is given by the owner of a right to another, for the use of that right, free from legal recourse.

Low dollar value: Procurement requirements that are generally less complex and a low risk, with an estimated total value below $25,000, including all applicable taxes

Maintenance: The cost of maintaining a property in efficient working condition.

Malware: Is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Is an umbrella term used to refer to a variety of forms of intrusive software including viruses, worms, Trojan horses and spyware.

Manage: To select, retrieve, view, create, review, copy, edit, update, action, share, track, distribute, re-use, save and delete any EPS record, EPS project information, metadata and metadata value.

Managed service: The practice of day-to-day management responsibilities and functions of business services provided by a service provider.

Master data: Data that describes the people (e.g., a customer, employee, supplier), places (e.g., a location, sales territory or office) and things (e.g., an account, product, asset or document set) involved in the business of an organization.

Master data management: Is a method to enable and link all of GC procurement critical data, Transactional, Operational and Analytical data, to one file, called a master file that provides a common point of reference. Master Data Management is set of technology enabled steps that will ensure uniformity, consistency and accuracy of procurement related shared data assets.

Material Resource: A room or equipment.

Metadata: Data that defines and describes other data and it is used to aid the identification, description, location or use of information systems, resources and elements.

Method of Payment: The method Canada will use to pay for work performed or goods delivered, such as all arrears (preferred), in advance, as a lot delivery or as each item are delivered. The following are types of methods of payment: Standard Payment Period and Interest on Overdue Account; Determination of the Method of Payment; Types of Method of Payment; Progress Payments; Advance Payments; Holdbacks.

Method of supply: A means of satisfying the procurement needs of a client for goods or services in the most economical and efficient manner, while respecting the objectives of government contracting to enhance access, competition, fairness and best value. In Canada, such agreements are also known as an SO, SA, or a Contract with a Task Authorization(s) (TA).

Method of Supply Limitation – Individual Supplier: The maximum dollar amount that a Supplier can receive in contracts / orders.

Method of Supply Limitation – Cumulative Limitation: The maximum dollar amount that all Suppliers can receive in contracts / orders.

Metrics: Measures of performance that observe progress and evaluate trends within an organization.

Milestone payment: A method of making a progress payment, which relates to a measurable and/or defined item or work package.

Mobile device: A transportable electronic device that is capable of receiving and transmitting electronic data wirelessly. Examples are Blackberry Smartphone and other secured Personal Digital Assistant (PDA).

Back to TOP

N

New Release: A system release, a version release, and interim release of licensed software, regardless of whether the Contractor refers to it as a "new release".

Non-functional requirement: A requirement that specifies criteria that can be used to determine the operation of a system, rather than specific behaviors.

Notice: An electronic advertisement that: solicits goods or services; indicates that a solicitation is being updated/changed; or announces a contract award.

Notification: A system generated message notifying a user of an action required (i.e. approve, deny) or that an action has been completed that requires attention.

Back to TOP

O

Open Data: Open Data is a philosophy and practice that makes data easily available in order to enable re-use of the data in new and unforeseen ways. http://open.canada.ca

Operational phase: The period that starts from the first day following the completion of the Implementation Phase.

Operations: The ability of an organization to meet its operational goals and commitments. Factors include the quality of the organizational structure, including skills, experience, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Operations Center: Contractor location that includes infrastructure and resources required for the centralized management and operation of the PWGSC

Operator: A person, under the control of the Contractor, which administers PWGSC EPS Service Infrastructure.

Order: A confirmed request by one party to another to buy, sell, deliver, or receive goods or services under specified terms and conditions. Refer to Purchase Order in this annex.

Order Selection Methodology: Business rules used to distribute Orders when there is more than one pre-qualified supplier offering the same goods/services under a Standing Offer or Contract with Task Authorizations.

Order Threshold: An order threshold is the maximum dollar amount that a user can issue an Order without seeking the approval of the Contracting Authority for the applicable Method of Supply. The Contracting Authority may also have a maximum order threshold.

Original Equipment Manufacturer: The manufacturer of the hardware, as evidenced by the name appearing on the hardware and on all accompanying documentation.

Organization: An organization is any institution, other than a Canadian government department, agency or crown corporation, holding or referring to a security clearance. The majority are commercial corporations, but other institutions are also included, such as university faculties, partnerships, consultants, and other levels of government and their agencies.

Back to TOP

P

Patch Management: Standardized methods and procedures to minimize the impact of Problems for PWGSC EPS Services.

Payment Method: Refer to Method of Payment in this annex.

Periodic User Satisfaction Sample Volume: Parameter to measure the distribution rate of User satisfaction surveys. User contacts who submitted a Service Request (with the exception of password reset Service Requests) or an Incident qualify to receive a survey once the Incident is Resolved or Service Request is completed (a “qualifying Service Desk contact”).

Phone Call Speed: The Phone Call Speed is the parameter to measure the time for the Service Desk to answer the phone. Measurement starts from the time the call enters the Service Desk wait queue to the time the call is answered by a Service Desk agent.

Platform: General purpose information systems components used to process and store electronic data, such as desktop computers, servers, network devices, and mobile devices. Platforms usually contain server hardware, storage hardware, utility hardware, software and operating systems.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure

including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Portal: A portal is a specially designed web page which brings information together from diverse sources in a uniform way. Usually, each information source gets its dedicated area on the page for displaying information; often, the user can configure which ones to display. Variants of portals include intranet "dashboards" for executives and managers.

Pricing Evaluation Framework: For the contracting officer to establish a price threshold where the supplier can increase or decrease their price, without seeking approval from the contracting officer (-30% + 30%). If the price they are proposing is not in this threshold it will trigger a notification to advise the contracting officer.

Privileged User: A User that is authorized to perform privilege operations for the PWGSC EPS Services.

Problem: Unknown cause of one or more incidents, often identified as a result of multiple similar incidents.

Problem Management: Standardized methods and procedures to minimize the impact of Problems.

Process: A collection of related, structured steps that produce a specific service or product (serve a particular goal). It often can be visualized with a flowchart as a sequence of activities with interleaving decision points or with a Process Matrix as a sequence of activities with relevance rules based on the data in the process.

Process Management: Is the ensemble of activities of planning and monitoring the performance of a business process. It is the application of knowledge, skills, tools, techniques and systems to define, visualize, measure, control, report and improve processes

Process map: A process map depicts and models business processes that are performed by users, roles or actors in an enterprise. Refer to Activity, Actor, Role, User and Workflow diagram definitions in this annex.

Procurement: The process of obtaining goods and services that includes the determination of requirements and acquisition from a supply system or by purchase from the trade.

Procurement Business Number (PBN): A unique identifier that is assigned to each supplier when they register in the Supplier Registration Information service, on the Buying and Selling Web site. It is based on the nine-digit Business Number that Canada Revenue Agency assigns to a supplier for tax matters related to business in Canada.

Procurement process: This process addresses the acquisition of goods and services, in the right quantity, at the right time, in the right place, at the best possible quality, cost and value, and from the responsive source. The complexity of the procurement process depends on many factors.

Production System: It implies real-time and real-data computer systems that are running in production environment used within GC that will interoperate, communicate, execute programs or transfer data with EPS in order to process GC procurement daily work and to accommodate the activities associated with the execution of one or more Systems in a manner that is fully exposed, made available to and supported for final and intended End Users of such Systems.

Productivity: A measure of how well resources are combined and utilized to achieve a particular desirable result.

Project Complexity and Risk Assessment (PCRA): Process and tools used within PWGSC to, initially upon receiving requisition and iteratively throughout procurement process, determine and establish procurement project level of complexity (i.e. 5 levels of Complexity) and assess and mitigate procurement project risk.

Project/Activity Management: Set of tools and methodologies that are readily available within solution for management of procurement projects and its related activities.

Proposal: An offer, submitted in response to a request from a contracting authority, which constitutes a solution to the problem, requirement or objective in the request.

Proprietary: Belonging to ownership; owned by a particular person; belonging or pertaining to a proprietor; relating to a certain owner or proprietor.

Protected Information: This refers to specific provisions of the *Access to Information Act* and the *Privacy Act* and applies to sensitive personal, private, and business information.

1) Protected A (low-sensitive): Applies to information that, if compromised, could reasonably be expected to cause injury outside the National Interest, e.g., disclosure of exact salary figures.
2) Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the National Interest, e.g., loss of reputation or competitive advantage.
3) Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the National Interest, e.g., loss of life.

Protocol: A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

Public Data: Information that covers or details publicly available information. Refer to Open Data in this annex.

Public Notice: Are announcements from all levels and branches of government, from businesses and from individuals. Public notices inform you about government actions, environmental conditions and economic changes.

Publishing Date: The date on which the tender notice becomes active and suppliers and general public are able to view the notice on Government Electronic Tendering Service (GETS).

PunchOut: It is part of a Catalogue Management system that connects a buyer to a supplier's external web site from within the EPS.

Purchase Description: A statement of requirements to identify and describe a particular product or service, but which may be less detailed than a specification. The description includes sufficient data to enable the supply and evaluation of the item either by means of reference to a specification or standard, or by the inclusion of critical performance data.

Purchase Order: A purchaser's written offer to a supplier, formally stating all terms and conditions of a proposed transaction, which is created in the procurement solution when a shopping cart is ordered. The purchase order contains all shopping cart items for a single supplier. The purchase order can be printed and sent to the supplier.

Purchasing: The buying process within the procurement cycle.

Purchasing Organization: The purchasing organization represents the procuring unit in a legal sense.

Public-Key Infrastructure (PKI): A comprehensive system required to provide public-key encryption and digital signature services across a wide variety of applications. An organization establishes and maintains a trustworthy networking environment by managing keys and certificates through a PKI.

Back to TOP

Q-R

Quality Assurance: A system of activities whose purpose is to provide assurance that the quality control is in fact being done effectively. For a specific product or service, this involves verification, audits and the evaluation of the quality factors that affect the specification, production, inspection and distribution.

Quality Control: This refers to a range of activities, to ensure and verify that the specific quality of the product or service has been met.
Quotation: A response to a Request for Quotation in regards to price and availability for goods and services.

Quote: Refer to Quotation in this annex.

Real-Time Data: Data that is active and is at the given point in time being worked on in the Solution.

Reasonable: What is fair, just, suitable and proper in the given circumstances of a case, that which is fit and appropriate to the end in view, and that which is according to reason, not immoderate or excessive

Receipt: An original document and electronic copy of a certified true copy showing the amount of expenditure and the date of a transaction as proof of payment.

Record: Information in any format created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Region of Delivery: The region where the goods or services being requested are to be delivered.

Reliability: The measures expressed of the ability of a product to function successfully when required, for the period required, in the specified environment.

Remedy: A right given to a party by law or by contract which that may exercise upon a default by the other contracting party, or upon the commission of a wrong by another party. It means any remedial right to which an aggrieved party is entitled with or without resort to a tribunal.

Release Management: Standardized methods and procedures for the integration and flow of development, testing, deployment, and support of PWGSC EPS Services.

Remote Access: Access to the PWGSC EPS Service Infrastructure through an external network (e.g., the Internet).

Repair: To restore (something damaged or broken) to good condition or working order.

Reporting: The generation of standard, custom or ad hoc reports, based on specific fields of required information that are displayed in the most suitable format. Refer to Business Intelligence (BI).

Repository: An electronic or physical location for safely storing or preserving information of use and value to the federal government.

Request for x (RFx): A term in the strategic sourcing and procurement landscape. It is a catch-all term that encompasses all references to a Request for Information (RFI), Request for Proposal (RFP), Request for Quotation (RFQ), Request for Supply Arrangement (RFSA), and Request for Standing Offer (RFSO).

Request for Information (RFI): An RFI or Letter of Interest is not open for bidding. The buyer is interested in receiving feedback from suppliers and may re-open or re-issue an opportunity at a later day.

Request for Proposal (RFP): A form of bid solicitation used where the selection of a supplier cannot be made solely on the basis of the lowest price. An RFP is used to procure the most cost-effective solution based upon evaluation criteria identified in the RFP.

Request for Quotation (RFSO): A solicitation document used to solicit standing offers. It must clearly state the requirement, the evaluation method and selection criteria, the call-up procedures, the ranking methodologies, whenever applicable, to be used for making call-ups against the authorized standing offer(s), and all terms and conditions applicable to the contract that is brought into effect, as a result of any call-up.

Request for Standing Offer (RFSA): A procurement tool established by PWGSC for use by clients that allows buyers to solicit bids from a pool of pre-qualified suppliers for specific requirements. The intent is to establish a framework to permit expeditious processing of individual bid solicitations which result in legally binding contracts for the goods and services described in those bid solicitations.

Request for Quotation (RFQ): A Solicitation document used to solicit bids for low dollar value requirements below $25,000.00, including all applicable taxes, from one or more suppliers. It is a request to bidders, which is evaluated with the objective of accepting the lowest-priced responsive quotation.

Requisition: A request to obtain materiel or services and authority to commit funds to cover the purchase.

Requisitioner: An internal user who has been given authority to submit electronic requests (Requisitions) for items or services.

Reverse e-Auction: An online reverse auction that takes place in real time. It gives suppliers the opportunity to bid against each other to improve their offers.

Resource Management: The process of using resources in the most efficient way possible. These resources can include tangible resources such as goods and equipment, financial resources, and labor resources such as employees

Responsive bid: A bid, tender, proposal or quotation that meets all the mandatory requirements stipulated in the solicitation document.

Right of First Refusal: The Government of Canada contacts the highest-ranked Supplier within the Standing Offer to determine if the requirement can be satisfied by that Supplier. If the highest-ranked Supplier is able to meet the requirement, a Call-up is made against the Standing Offer. If that Supplier is unable to meet the requirement, the government will contact the next highest ranked Supplier.

Role: A set of responsibilities assigned to an individual or group for the purposes of performing a specific job function, activity or task. A role determines the access rights and permissions granted to an individual or group. Reference Access rights in this annex.

Back to TOP

S

Scalability: Scalability is the ability of a system, network, or process to handle a growing workload in a capable manner or its ability to be enlarged to accommodate that growth. This capability allows computer equipment and software programs to grow over time, rather than needing to be replaced. A scalable network should be able to support additional connections without data transfers slowing down. In each instance, scalable hardware can expand to meet increasing demands. While all hardware and software have some limitations, scalable equipment and programs offer a long-term advantage over those that are not designed to grow over time.

Schema: The structure that defines the organization of data in a database.

Scorecard: Is a strategy performance management tool - a semi-standard structured report, supported by design methods and automation tools that can be used by managers to keep track of the execution of activities by the staff within their control and to monitor the consequences arising from these actions

Sealed Bid: A sealed bid is a document enclosed in a sealed envelope and is submitted in response to invitation to bid. Sealed bids received up to deadline date are generally opened at a stated time and place usually in the presence of anyone who may wish to be present and evaluated for award of a contract.

Secure Access: Refers to the ability to permit or deny user access to resources within the solution.

Secure Perimeter: Logical and physical boundary around network accessible resources and information, which is controlled and protected against unauthorized access from outside of the boundary.

Security Assessment: The on-going process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security.

Security Authorization: The on-going process of obtaining and maintaining official management decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk of relying on the information system to support a set of business activities based on the implementation of an agreed-upon set of security controls, and the results of continuous security assessment.

Security Deposit: The deposit by the bidder/contractor of securities, including government guaranteed bonds, bills of exchange and irrevocable standby letters of credit, which the contracting authority may convert to complete the bidder's/contractor's obligations.

Security Posture: A characteristic of an information system that represents the ability of implemented security controls to satisfy the business needs for security and counter a selected threat environment.

Security Requirements Check List (SRCL): A form that is used to identify PROTECTED or CLASSIFIED security requirements associated with a Contract.

Service Delivery Point (SDP): Physical location in a building where the solution is implemented.

Service Desk Availability: Service Desk Availability refers to the required time frames during which services provided by the Service Desk must be available to Users.

Service Desk Reporting: Service Desk Reporting relate to the activities associated with the preparation of and access to Service Desk reports that are based on defined criteria.

Service Desk User Satisfaction Service Level: Parameter to measure User satisfaction with the services provided by the Contractor.

Service Oriented Architecture: A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product or technology.

Service procurement: This discipline supports managing and streamlining procurement and contracting related to external workers. Service procurement addresses the full life cycle of service acquisition, from requisition to monitoring, with a focus on reducing the organizational cost of incorporating an external workforce. It includes requirements specification, selection and approval workflows, requisitioning, order monitoring and aftercare.

Shopping Cart: An electronic "basket" used for holding items until the Requisitioner instructs the system to enter (save) them into a requisition. The shopping cart serves as the intermediary step between the user searching a catalogue and placing the order through a requisition.

Shopping Cart Request: A document that has a collection of items selected from available catalogue items.

Slice and Dice: Is mostly used in Business Analysis for dividing a quantity of information up into smaller parts, especially in order to analyze it more closely or in different ways.

Snapshot: A view of data at a particular moment in time.

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation Number: An internal procurement code that is assigned to an opportunity that is generated through EPS.

Sole Source: The supply of a good or service that is available from only one supplier. A sole source contract implies that there is only one supplier that can fulfill the requirement and that any attempt to obtain bids would only result in one supplier being able to meet the need.

Solution: The e-Procurement Solution.

Solution User Data: Includes Account, Notifications, Customized views and filters.

Sourcing event: The procurement process may involve a sourcing event for a particular good or service that meets a requirement and/or follows a prescribed workflow. The end result is the selection of a supplier and the award of a Contract.

Spend: The process of collecting, cleansing, classifying and analyzing spend information with the purpose of addressing expenditures for active Contracts, reducing procurement costs, and monitoring compliance.

Spend analysis: A software- and service-based technique for collecting, cleansing, classifying and analyzing spend data. Refer to Analytics, Dashboard, Business intelligence and Reporting definitions in this annex.

Standard: A formal statement of requirements established by authority, custom or general consent of those affected, and intended for general recurrent use. Normally, a standard is developed through a consensus process by a committee widely representative of major interests and is published by an accredited standards-writing agency, as determined by the Standards Council of Canada or recognized standards-issuing agency.

Standard Procurement: A standard procurement has the characteristics of judgment, review, and assessment. The procurement is based on the process of finding a solution to a requirement using existing technology and knowledge. Evaluation methods have to be defined, and may use pre-established strategies. The procurement process is established and understood though it can be complicated (many details or factors). Control is within the department's domain of authority. Contract administration is predictable and established. There may be a medium level of risk

Standing Offer (SO): A standing offer is an offer from a potential supplier to provide goods and/or services at pre-arranged prices, under set terms and conditions, when and if required. It is not a contract until the government issues a "call-up" against the standing offer. The government is under no actual obligation to purchase until that time.

Stakeholder: An individual or a group that has a stake or interest in the development or purchase of a system, product or service. A group or individual with a relationship to the change, need, or the solution.

Statement of Work (SOW): The part of a Contract which contains a comprehensive, narrative description of the work required. The SOW defines tasks to be accomplished or services to be delivered in clear, concise and meaningful terms. It also stipulates the services or deliverables that are required to fulfill a Contract.

Statement of Work Builder: Provides the user with step-by-step guidance to develop a narrative description of the required work. The builder would ask for answers to guide the user and control the contents and final creation of the statement of work (SOW) document.

Storage: A function which involves the receipt of an item, putting it away for safekeeping and subsequent retrieval, when required for use, sale or disposal.

Strategic Sourcing: In opposition to transactional purchasing. To be involved in the definition of requirements, the client's satisfaction, the value creation process.

Subcontractor: One who takes portion of a contract from principal contractor or another subcontractor.

Superseded Clauses: Previous version of clauses which have been archived but can be referenced if needed.

Supplier: Is someone who provides goods or services. Represents External users of the EPS that will be using the solution to offer their services in response to various tenders published by GC.

Supplier credentials management: Managing the credentials of a supplier involves gathering, tracking (e.g., missing or expiring documents), amalgamating and storing evidence (e.g., certifications, legal documents, quality assessments, facility and/or individual security clearances, product test results, statements of service integrity and testimonial material) regarding the current capability and experience of a supplier. In most cases, supplier credentials are provided by the supplier in a bid.

Supplier performance: Managing supplier performance ensures that previous experience with a supplier will meet the requirements and expectations defined in a Contract. Upon the award of a Contract, the focus is on managing the actual performance of a supplier, the identification of performance gaps, and agreement on actions required to achieve the desired performance level.

Supplier portal: A website that offers a broad array of resources for suppliers to participate in the GC procurement process.

Supplier Relationship Management (SRM): A function that involves managing day-to-day interactions and end-to-end activities with a supplier throughout the lifecycle of a project, product or service.

Supplier repository: A library of electronic documents and specific information linked to a procurement file in a secure, effective and self-service environment. It enables the central management and auto-generation of re-usable, supplier-related information. This repository ensures that all supplier-related information is accessible to authorized personnel on an as- and when-required basis.

Supplier risk management: Encompasses all tools used to model, map and track the potential of an undesired event associated with a supplier which may have a detrimental effect on a purchasing operation and/or outcome. Supplier risk management includes the ability to monitor Contract compliance, identify risk sources (i.e., frameworks for applying a systematic approach to risk management), develop risk indicators, subsequently manage and monitor operational supply risk, and implement supplier corrective action as required.

Supplier Selection Methodology: Are the methodologies used to determine: the minimum number of eligible pre-qualified Suppliers to be invited, the minimum number of calendar days for the RFx posting, how Suppliers are selected (e.g. random, rotational) and the Publishing requirements (e.g. direct invitation vs. published on GETS). Typically there are different rules (tiers) based on dollar value.

Supply Arrangements (SA): Is a method of supply used by Public Works and Government Services Canada (PWGSC) to procure goods and services. Like standing offers, it is not a contract and neither party is legally bound as a result of signing a supply arrangement alone.

Back to TOP

T

Task Authorization: A task authorization (TA) is a structured administrative tool that enables PWGSC or a client to authorize work by a contractor on an "as and when requested" basis in accordance with the conditions of the contract. TAs are not individual contracts.

Taxonomies: Is a way to classify and assign a structure to information.

Technology Architecture : Technology Architecture is the activities associated with the design and development of the IT infrastructure and tools that support the IT Service Towers.

Temporary Help Services: Services provided under contract to the government for assignments in which employees of a supplier work under the direction of public servants.

Tender notice: A publicly available notice that a solicitation opportunity is available.

Threat and Risk Assessment (TRA): Structured process designed to identify risks and provide recommendations for risk mitigation through analysis of system / service critical assets, potential threat events / scenarios, and inherent vulnerabilities.

Traceability: The ability to verify the history, location, or application of an item by means of documented recorded identification.

Train-the-Trainer: A training program designed to teach participants how to deliver instructor-led, hands-on training for the service solution to end users.

Trainer: An individual who is responsible for teaching details relating to a service(s).

Transaction: Is a financial or technical online electronic process and information exchange between two or more parties that results in obtaining a desirable outcome. In procurement transaction is defined as a set of steps and functions that lead to an exchange or transfer of funds, goods, services or construction. The steps may including description of requirements, selection and solicitation of sources, preparation and award of contract, and all phases of contract administration which includes paying for an item or service.

Transactional data: Data that describe an internal or external event or transaction that takes place as an organization conducts its business (e.g., a sales order, invoice, purchase order, shipping document, credit card payment, ect.).

Transactional Procurement: Purchasing which is only a support function dealing more with administration (ordering, tracking, invoicing) than strategy**.**

Back to TOP

U

Unauthorized Access: When an entity gains unauthorized access to a system in order to commit another crime such as destroying information contained in that system. Examples include: infiltration, compromise, hacking, privilege escalation and unauthorized access/privilege.

Use case: An analysis tool that describes the tasks that a system, solution or service performs for an actor and the goals that the actor will achieve as a result of the process. It should yield and depict an observable and measurable result that is of value to the actor.

User: An individual authorized by the Client who uses a particular system, product, solution or service. A user may also be someone who assumes a particular role in an organization and performs designated functions within a business or system domain.

User Interface (UI): Is everything designed into an information device with which a human being may interact -- including display screen, keyboard, mouse, light pen, the appearance of a desktop, illuminated characters, help messages, and how an application program or a Web site invites interaction and responds to it. The user interface can arguably include the total "user experience," which may include the aesthetic appearance of the device, response time, and the content that is presented to the user within the context of the user interface.

User profile: Is a record of user-specific data that defines the user's working environment and roles.

Back to TOP

V

Vendor: An entity that provides goods and services to the specific client. Refer to supplier in this annex.

Voice Mail Response Time: Parameter to measure the time for EPS Service Provider to respond to voice mails received at the Service Desk. Time is measured from the time the voice mail is received by the voice

mail system to the time the voice-mail is responded to and the Service Desk agent's response is logged in the System.

Back to TOP

W

Web Services: A standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

Wizard: A software wizard is a user interface element that presents a user with a sequence of dialog boxes that lead the user through a series of well-defined steps. Tasks that are complex, infrequently performed, or unfamiliar may be easier to perform using a wizard (e.g. User Configuration).

Workflow: The routing of a procurement file along a prescribed workflow (or process path) associated with a particular service or good. Workflow is configurable based on commodities, business rules, policies and their specific steps (e.g., collaboration, review, validation, bid evaluation and approval).

Workload Management: The ability to assign, schedule and manage tasks and schedules for purchasing staff, including the ability to assign workers to service lines, manage availability, level the volume and type of work tasks across staff resources as efficiently as possible, and in line with predetermined service-level objectives.

Back to TOP

X-Y-Z

ZIP folder: An electronic folder of compressed files.

Back to TOP

ANNEX 6

ACRONYMS

1.0 ACRONYMS

This section outlines acronyms that are found throughout this solicitation. This section should be used in conjunction with Section 5, "Glossary of Terms". This document also complements the contractual terms and conditions that will appear in the solicitation and resulting contract.

Acronym	Description
ABAC	Attribute-Based Access Control
ACAN	Advance Contract Award Notice
ADM	Assistant Deputy Minister
AIT	Agreement on Internal Trade
AB	Acquisitions Branch
AP	Acquisition Program
API	Application Programming Interface
BC	Business Continuity
BCP	Business Continuity Plan
BF	Bring Forward
BI	Business Intelligence
BIA	Business Impact Analysis
BN	Business Number
BPEL	Business Process Execution Language
BPM	Business Process Management
CA	Contracting Authority
CAB	Change Advisory Board
CAD	Computer-Aided Design
CAN	Contract Award Notice
CDO	Collaboration Data Objects
CEDI	Common Enterprise Data Initiative
CIOB	Chief Information Officer Branch
CIOC	Chief Information Officer Council
CIs	Configurable Items
CIS	Client Information System
CISD	Canadian Industrial Security Directorate
CITT	Canadian International Trade Tribunal
CLF2	Common Look and Feel for the Internet 2.0
CLCA	Comprehensive Land Claims Agreements
CLM	Contract Lifecycle Management
CMDB	Configuration Management Database
COBIT	Control Objectives for Information and Related Technology
COTS	Commercial Off-the-Shelf
CPI	Consumer Price Index
CPU	Central Processing Unit

Acronym	Description
CRA	Canada Revenue Agency
CRL	Certificate Revocation List
CSE	Communication Security Establishment
CSI	Construction Specific Institute
CSS	Client Service Strategy
CSV	Comma Separated Values
CTO	Chief Technology Officer
CWBS	Contract Work Breakdown Structure
CWG	Catalogue Working Group
cXML	Commercial eXtensible Markup Language
DFMS	Departmental Financial & Materiel Management Systems
DHS	Definitive Hardware Store
DSL	Definitive Software Library
DM	Deputy Minister
DMPS	Defence and Major Projects Sector (within the AB)
DND	Department of National Defence
DOC	Departmental Oversight Committee
DR	Disaster Recovery
DSP	Drawing and Specification Packages
DW	Data Warehouse
EDI	Electronic Data Interchange
EPS	e-Procurement Solution
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
EST	Eastern Standard Time
ETL	Extract, Transform and Load (ETL)
FMS	Financial Management Sector
FMT	Financial Management Transformation
FPOC	First Point of Contact
FCC	Foreign Currency Component
FSC	Forward Schedule of Changes
FY	Fiscal Year
GC	Government of Canada
GCDOCS	Government of Canada Electronic Document Record Management Solution
GCIF	Government of Canada Interoperability Framework
GCR	Government Contract Regulation
GETS	Government Electronic Tendering Service
GL	General Ledger
GSIN	Goods and Services Identification Number
HTML	HyperText Markup Language

Acronym	Description
HTTP	HyperText Transfer Protocol
IAM	Identity and Access Management
ICAM	Identity, Credential and Access Management
ICAS	Identity, Credential and Access Solution
ID	Identification
IP	Intellectual Property
ISO	International Standards Organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSB	Information Technology Security Bulletin
ITSG	Information Technology Security Guidance
ITSM	IT Service Management
ITQ	Invitation to Qualify
ITT	Invitation to Tender
IVR	Interactive Voice Response
Java EE	Java (platform) Enterprise Edition (architecture)
JV	Joint Venture
JSON	JavaScript Object Notation
KM	Knowledge Management
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LIS	List of Interested Suppliers
LOI	Letter of Intent
LQS	List of Qualified Suppliers
MAPI	Mail Application Program Interface
MSRP	Message Session Relay Protocol (or Manufacturer's Suggested Retail Price)
NAFTA	North American Free Trade Agreement
NATO	North Atlantic Treaty Organization
NCR	National Capital Region
NISO	National Individual Standing Offer
NIST	National Institute of Standards and Technology
NMSO	National Master Standing Offer
NTD	Network Transit Delay
OEM	Original Equipment Manufacturer
OLAP	On-line Analytical Processing
P2P	Procure-to-Pay
PA	Performance Agreement
PBN	Procurement Business Number
PDF	Portable Document Format

Acronym	Description
PDR	Packet Delivery Ratio
PIPEDA	Personal Information Protection and Electronic Documents Act
PKI	Public Key Infrastructure
PO	Purchase Order
PSAB	Procurement Strategy for Aboriginal Business
PWGSC	Public Works & Government Services Canada
RACI	Responsible, Accountable, Consulted, Informed
RAM	Random-access memory
REST	Representational State Transfer
RFC	Request for Change
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quote
RFSA	Request for Supply Arrangement
RFSO	Request for Standing Offer
RFx	Request For "x"
RRR	Review and Refine Requirements (process)
RSS	Really Simple Syndication
SAs	Supply Arrangements
SaaS	Software as a Service
SAML 2.0	Security Assertion Markup Language
SAP	Systems, Applications and Products
SDK	Software Development Kit
SLA	Service Level Agreement
SLR	Service Level Requirements
SME	Small and medium-sized enterprises or Subject Matter Expert
SOs	Standing Offers
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SOS	Statement of Sensitivity
SOW	Statement of Work
SRCL	Security Requirements Check List
SRM	Supplier Relationship Management
SSC	Shared Services Canada
SSO	Single Sign-On
TAs	Task Authorizations
TB	Treasury Board
TBD	To be Determined
TBS	Treasury Board Secretariat

Acronym	Description
TR&R	Technology Refreshment and Replenishment
UAT	User Acceptance Testing
UBL	Universal Business Language
UNSPSC	United Nations Standard Products and Services Code
VIP	Very Important Person
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

ANNEX 7

TASK AUTHORIZATION FORM

Form Instructions

This template provides the basis for the Task Authorizations, as detailed in the resulting contract clauses. Task Authorizations authorize work to be performed, in accordance with the labour categories defined in "Annex 1 – SOW, Part 7 Optional Services" and the associated rates defined in "Annex 3 – Price Schedule".

Commentary or guidance on completing a section of the form are identified in the brackets <>, and should be removed when completing the form.

All Task Authorizations should have a unique number to identify them.

e-Procurement Solution (EPS)

Please provide the appropriate unique identification number and title:

Task Authorization (TA) Number

Title:_____

Approvals

	Name	Signature	Date
Prepared by:			
Approved by Project Authority:			
Approved by Contracting Authority:			
Accepted by Contractor:			

Remarks:

<Enter introductory remarks>

1 Background Information

<Enter background information.>

2 Overview of Requirement

<Provide a high level description of requirement and indicate the labour category.>

3 Objective and Scope

<Define the objectives and scope of this TA.>

4 Requirements

<Provide a description of the requirements that will be addressed by this TA.>

5 Project Plan

<Provide a high level plan outlining the project steps, timelines, resource requirements and interdependencies.>

6 Roles and Responsibilities

<Identify the roles and responsibilities associated with this TA.>

7 Project Deliverables and Milestones

<Provide a description of the project deliverables and identify major milestones with dates.>

8 Assumptions and Constraints

<Detail any assumptions and constraints associated with the completion of this TA.>

9 Cost Detail

<Provide detailed costing to support justification for this TA.>

10 Acceptance Criteria

<Provide a description of the criteria that must be met in order for the work completed under this TA to be accepted and payment authorized.>

ATTACHMENT 1 TO PART 2:

EPS BUSINESS PROCESS MODELING METHODOLOGY

Table of Contents

1. Business Process Information Intent & Context

The Business Process Information in this attachment is supplemental information to assist Bidders in understanding the business process flow supporting the SOW requirements. However, the material in this attachment is not intended to represent the process architecture for an EPS future state. The inclusion of this information in the bid solicitation does not represent a commitment by Canada that Canada's EPS future state will be consistent with this information. It is provided purely for information purposes and will not form part of the resulting Contract.

The Business Process flow depicted in this document reflects possible scenario(s) with respect to the sequence and order of occurrence of any given activity. The sequential nature of the Business Process flow is subject to the characteristics of the procurement process of any given commodity at any point in time in the process and is subject to change given the particular conditions, criteria and nuances of a commodity's procurement. Therefore, some process activities depicted in this document may actually occur in a different stage, in parallel or simultaneously rather than sequentially. This is especially the case for (1) procurement complexity & risk assessments and (2) procurement planning approvals. The stage in the general process where these particular events may occur is subject to change in response to the specifics of the procurement of a commodity. The only exception is any process activity or event whose sequence or order of occurrence is governed by legislation, trade agreements or policy.

2. Additional General Contextual Information

For additional context, the following provides high level general information about the Business Process flow:

2.1. **Procurement Lifecycle Flexibilities**: The Process Flows are built on the premise of some regularity and consistency in the chronology of steps a client will go through for the procurement process. However, as with all processes, there are often exceptions to the rule and exceptional circumstances that require process management to step outside of the standard practice. The EPS must be built to accommodate such instances, including flexibility in management processes and systems functionality.

2.2. **Varied System Interfaces:** Since there are multiple delivery partners participating in procurement, there is also a wide array of systems and processes that must work together in order to deliver the program and provide the necessary information to each participating delivery partner. Ongoing system flexibility in the overall solution architecture, with the ability to receive input from and output to the systems involved is key to successfully delivering the EPS. Additional details are described in Part 5.

2.3. **Changing Environment:** Governments frequently introduce changes and new measures to the procurement process, impacting the way procurement is delivered and administered. A strong change management framework combined with a flexible e-enabled solution will be necessary to ensure that all required changes are implemented on time in an effective and efficient manner.

2.4. **Communications:** There are multiple delivery partners for the EPS and there are also a number of interested stakeholder groups and client types. Communications flexibility is important in order to satisfy requests for information from all these groups.

2.5. High Quality, Measurable Service: EPS and its delivery partners are accountable to the public for efficient operations, expenditures and ensuring the safety and protection of information. From a client perspective, procurement provides essential services which clients require to deliver on their operational mandates. It is important that the Contractor be able to demonstrate efficient, accurate service in a measurable manner.

2.6. Information Flow: Parliament, Government of Canada officials, stakeholders, and Canadians all require information that relates to procurement. Data and information made available through EPS needs to be comprehensive, timely and accurate in order to support an enhanced focus on accountability, reporting and analysis of information.

2.7. Stewardship: the Government of Canada is accountable to the public to ensure service delivery is conducted in a fashion that protects their privacy rights. Systems and services will incorporate adequate safeguards and mitigations to privacy rights.

3. Purpose of the Document

The primary purpose of this document is to summarize the draft business process information for the procurement process as it pertains to the scope of the e-procurement solution (EPS).

4. Assumptions

The assumptions that pertain specifically to this document and its content are:

a. This document and its accompanying business process models reflect initial draft business process information for the procurement process (as it pertains to the scope of EPS) based on sources such as previous as-is business process information and subject matter expert (SME) working groups
b. The business process information in this document is meant to reflect a possible future procurement business process state conceptualized in the context of EPS as accurately as possible given all current knowledge and unknowns of the scope and transformation opportunities of the EPS solution. Therefore it does not reflect specific EPS tool functionality but rather where/how the EPS tool solution can be incorporated into the procurement business process.
c. The business process analysis used in this modeling exercise is based on traditional business process modelling and analysis conventions of working from as-is model information and SME working group output to determine what existing processes will change and what new processes need to be added as a result of transformation. Therefore, the process models in this document do not reflect system process details but business process details for processes that are candidates for change. Any process activity not governed by legislation, trade agreements or policy are candidates for transformational change.
d. The audience of this document is knowledgeable of traditional business process modeling conventions.
e. The Business Process flow depicted in this document reflects possible scenario(s) with respect to the sequence and order of occurrence of any given activity. The sequential nature of the Business Process flow is subject to the characteristics of the procurement process of any given commodity at any point in time in the process and is subject to change given the particular conditions, criteria

and nuances of a commodity's procurement. Therefore, some process activities depicted in this document may actually occur in a different stage, in parallel or simultaneously rather than sequentially. This is especially the case for (1) procurement complexity & risk assessments and (2) procurement planning approvals. The stage in the general process where these particular events may occur is subject to change in response to the specifics of the procurement of a commodity. The only exception is any process activity or event whose sequence or order of occurrence is governed by legislation, trade agreements or policy.

5. Level 0 Business Process Models and Descriptions

Process Model

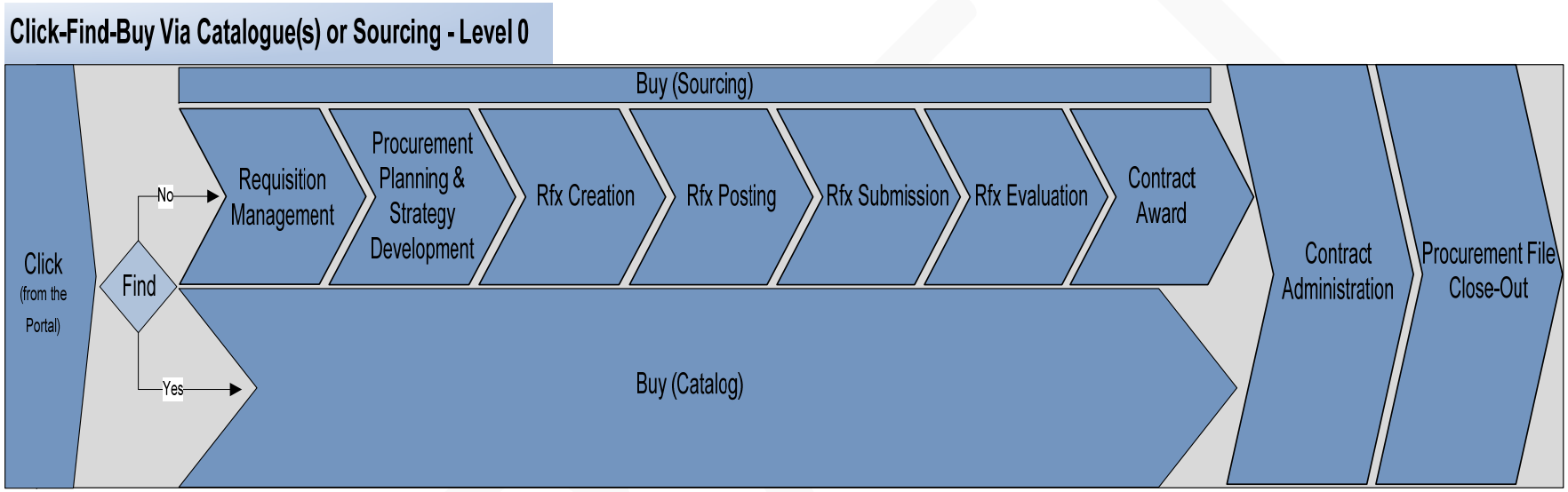


Figure 1 - Level 0 Click-Find-Buy Business Process Model

Process Description

This diagram represents the basic process of Click, Find and Buying the latter of which can occur via catalogues or via sourcing.

Lower Level Business Process Models and Descriptions

The following lower level process information (e.g. levels 1, 2, 3 and 4) that accompanies the process models is described by:

(a) **Summary Descriptions**: This is a summary description of the purpose of the business process and its pertinent steps and:

(b) **Process Model Flow Narratives**: This is a textual description of the flow of the process model to ease with understanding and reviewing the graphical process model

6. Level 1 Business Process Models and Descriptions

6.1. Click-Find-Buy

Process Model

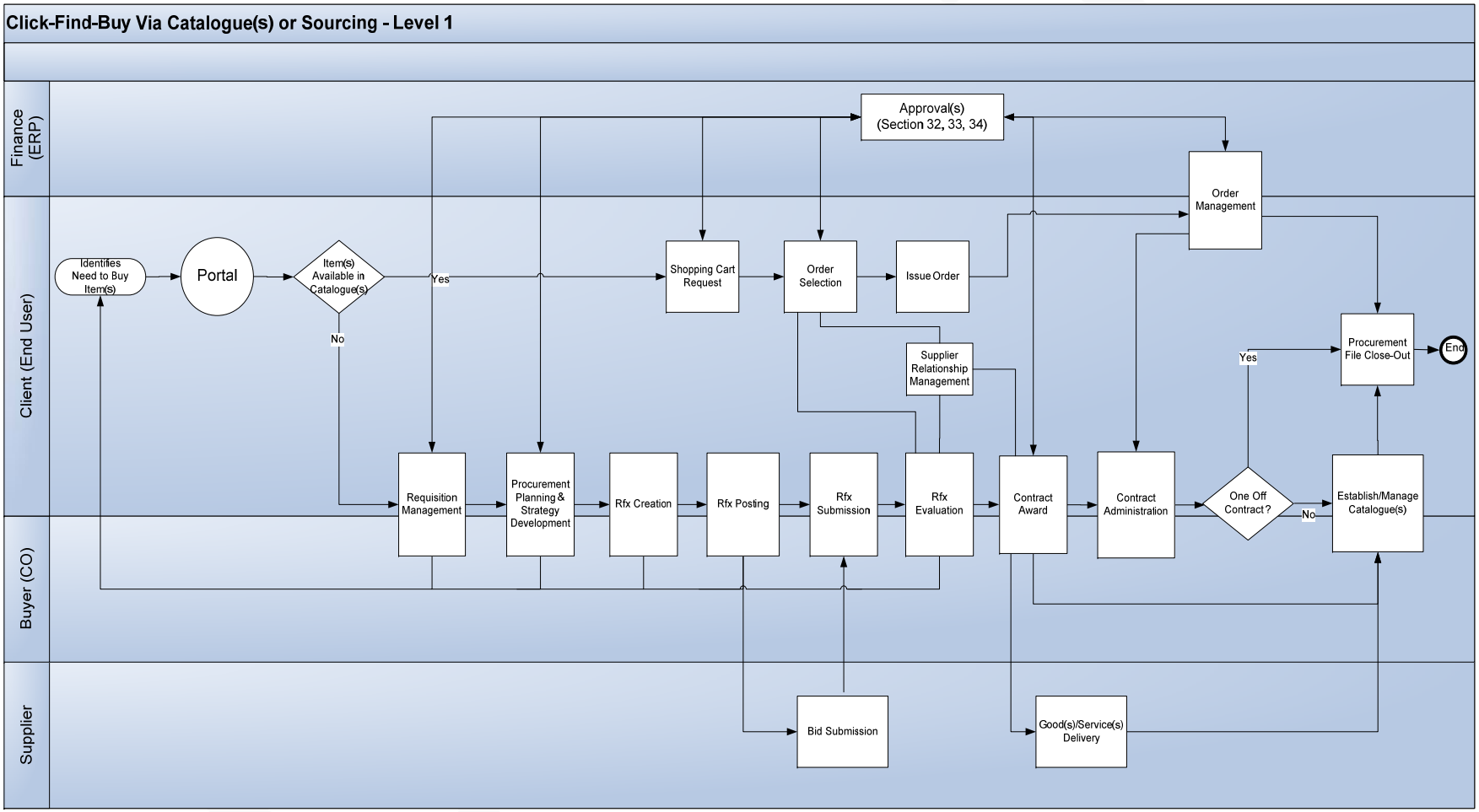


Figure 2 - Level 1 Click-Find-Buy Business Process Model

Process Description

Click-Find-Buy Via Catalogue(s) or Sourcing	
Summary Description	The purpose of the Click-Find-Buy level 0 process is mainly to depict the two choices of procurement available in the EPS solution, namely via one or more catalogues or the typical sourcing process. The context of this sub-process includes: • One and two phase procurement • Simple catalogue procurement • Simple and complex sourcing procurement • Procurement of all commodities available in the scope of EPS including professional services The basic steps in this level 1 process includes: • Clients initially searching one or more catalogues in the EPS solution to determine if their procurement needs can be satisfied by catalogue availability to which they have access to, • Clients completing their procurement via a catalogue purchase or a sourcing process procurement
Process Model Flow Narrative	The following process flow narrative pertains to Figure 2 : 1. The Client identifies a need to purchase 1 or more items of 1 or more different commodities from 1 or more catalogues. 2. From the Portal, using the catalogue(s) they have access to, the Client searches for their desired items. A successful search result confirms availability and pricing of some or all of their desired items. 3. Based on the Client deciding to accept the results of a successful search, they decide to complete their catalog purchase by completing and submitting their order, obtaining approval for the purchase, receiving delivery of their desired items and finally completing payment for their order. 4. Alternatively, based on either, an unsuccessful search result, or the Client deciding not to accept the results of a successful search, the Client decides to proceed with the procurement using the sourcing process. 5. During either of a catalogue or sourced procurement, the Supplier submits bids in the sourcing process & delivers ordered goods/services. As well, Finance completes financial approvals as per sections 32, 33, 41 & 44 of the GC Financial Administration Act (FAA) using the ERP of choice or EPS. 6. Upon completion of either method of procurement for the Clients desired items, using the EPS solution, the Client closes the procurement file and the process ends. 7. During the procurement process using either catalogues or sourcing, Supplier Performance is tracked, monitored and updated.

7. CATALOGUE PROCUREMENT

7.1. Level 2 Business Process Models and Descriptions

a. Catalogue Management

Process Model

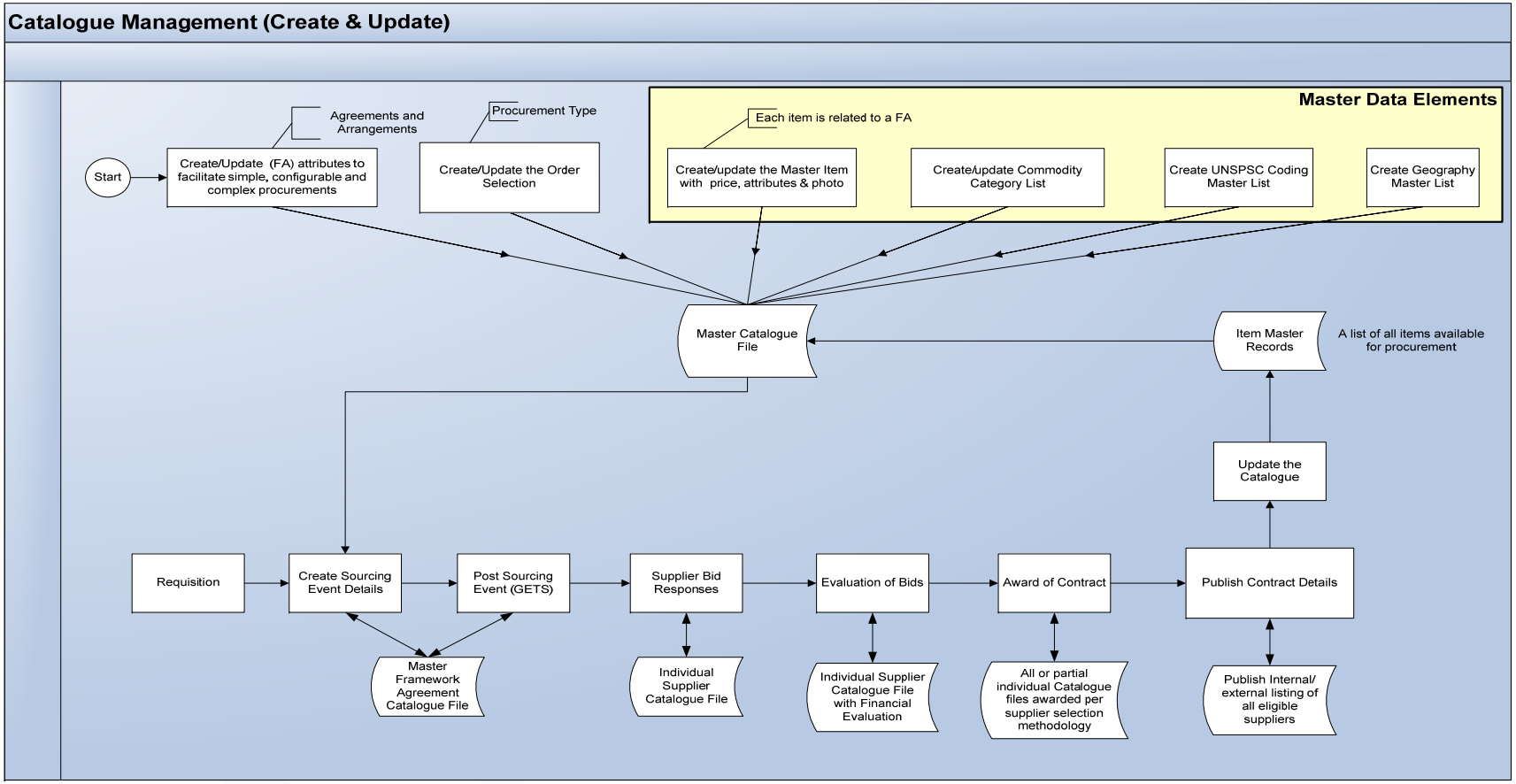


Figure 3 - Level 2 Catalogue Management Business Process Model

Process Description

Catalogue Management - Framework Agreement and Catalogue Creation	
Summary Description	The purpose of the Catalogue Management process consists of creating/updating a catalogue and/or a Framework Agreement within Catalogue Management.
Process Narrative	A Framework Agreement is made up of two distinct components: a) A Framework Agreement (FA) is the overarching agreement between the Government of Canada and the pre-qualified supplier(s) for the particular goods and services covered by the Framework Agreement. b) Catalogue Information – is the detailed information about the goods and services The purpose of catalogue information is to allow a Contracting Officer (CO) to create a repository of all relevant product attributes from a manufacturing part number, a description, a color, to tiered geographical pricing of a series of goods and services that prospective Suppliers will provide as a result of a sourcing event. Catalogue Information attributes are available from various master data attribute groups (e.g. geographic regions, taxonomies, and product attributes) to ensure the consistency of data. As a result of a sourcing event, the information contained in each individual Supplier's catalogue will be evaluated in accordance with technical and financial evaluation processes articulated in a sourcing event. As a result, only compliant information from Individual Supplier's catalogue information will be allowed up to the maximum number of Suppliers as per the supplier order selection and potentially made available for ordering in EPS. In the creation of a Framework Agreement, the Contracting Officer will identify all of the terms and conditions, including the order selection, order thresholds, and authorized organizations/users.

Input	**Description**
Data pertaining to an item	Item description, attribute, cost and link to another similar item
Data pertaining to an agreement and associated order selection	Term and conditions for all agreements with suppliers
Order Selection	The process in which available Orders are offered to pre-qualified Suppliers under a Framework Agreement.
Output	**Description**

Data to create/update catalogue	A new or updated catalogue was created for procurement purposes

b. Maintain the Catalogue

Process Model

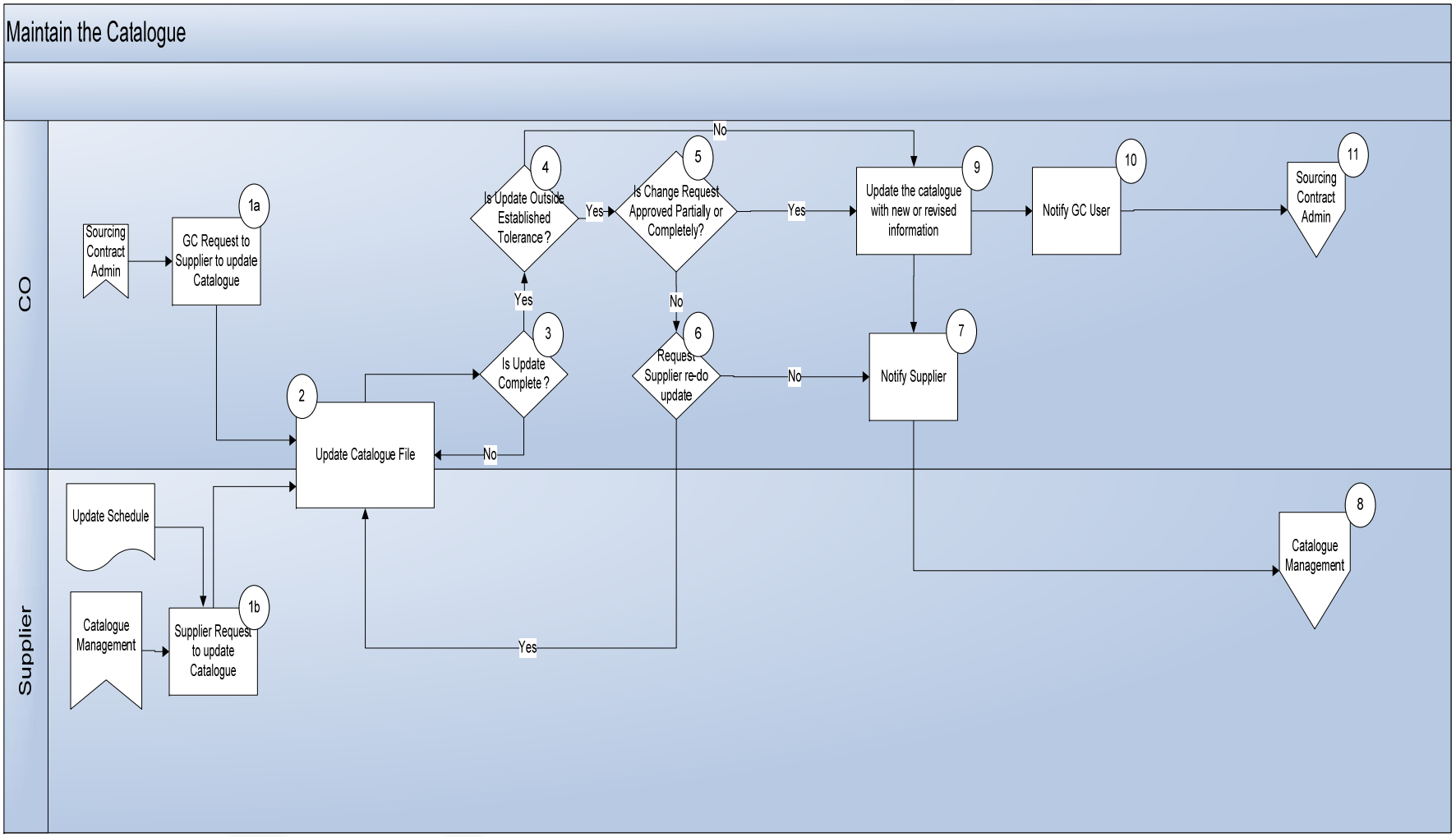


Figure 4 - Level 2 Maintain Catalogue Business Process Model

Process Description

Maintain the Catalogue	
Summary Description	The purpose of the Maintain the Catalogue process is to: • Update the Catalogue File • Update the Catalogue with new/revised information • Notify appropriate users of changes The Catalogue may be updated at various stages throughout the process. The Catalogue may be updated for various reasons (e.g. changing the name of a good/service, adding a good/service).
Process Narrative ***Actors:*** • ***GC Contracting Officer*** • **Supplier**	The following process flow narrative pertains to Figure 4: 1. Two possible methods by which the catalogue may be updated include, online and document upload. A Catalogue update can be either initiated by: a. A Government of Canada Contracting Officer as part of either an ad-hoc request. The CO has a reason/need to update the catalogue. b. A pre-established schedule or at the request of the Supplier (e.g. the supplier is no longer selling an item, or is changing the price). 2. The CO can complete the request to update the Catalogue (e.g. administrative changes, pricing updates). The Supplier can request to update the Catalogue information (e.g. pricing updates, removing obsolete items). 3. The CO checks whether or not the update is complete. If the update to the Catalogue is not complete, the Catalogue is updated again. 4. If the Catalogue update is complete, the CO determines if the change request is outside the tolerance (e.g. price update, discount percentage). 5. If yes, the CO is asked whether or not the change request is approved partially or completely. 6. If the change request is not approved, the CO Requests the Supplier to re-update their request. One option is to for the Supplier to re-update the Catalogue. 7. The other option is to notify the supplier of the incomplete Catalogue update. 8. The process returns to Catalogue Management. 9. If the change request is approved or if the Catalogue update is not outside the established tolerance, the Catalogue is updated with the new or revised information. 10. The CO notifies the GC User of a successful update to the Catalogue.

	11. The process returns to Sourcing Contract Administration

Input	Description
Change Updates	New catalogue information from the supplier
Output	**Description**
Reject notice	The CO has decided not to update the catalogue and is notifying the requester with a reason for rejection.
Updated catalogue record	The catalogue record is updated with the new information.
Change notification	The notification to the requester that the change has been made.

Business Rules

The Maintain the Catalogue business process is governed by the following rules:

1. On a periodic basis (e.g. yearly, weekly, monthly), the CO may update the catalogue.
2. The CO may create specific rules to update the catalogue/framework agreement. In fact, the CO can configure tolerances to limit changes to the catalogue /framework agreement (e.g. price discount/adjustment, inclusion of all or some categories).
3. Scheduling of updates may occur where the CO will not have to approve each catalog on a case-by-case basis (e.g. 70% of updates go through auto tolerance, but 30% are/will not be completed on time)

c. Shopping Cart Request

Process Model

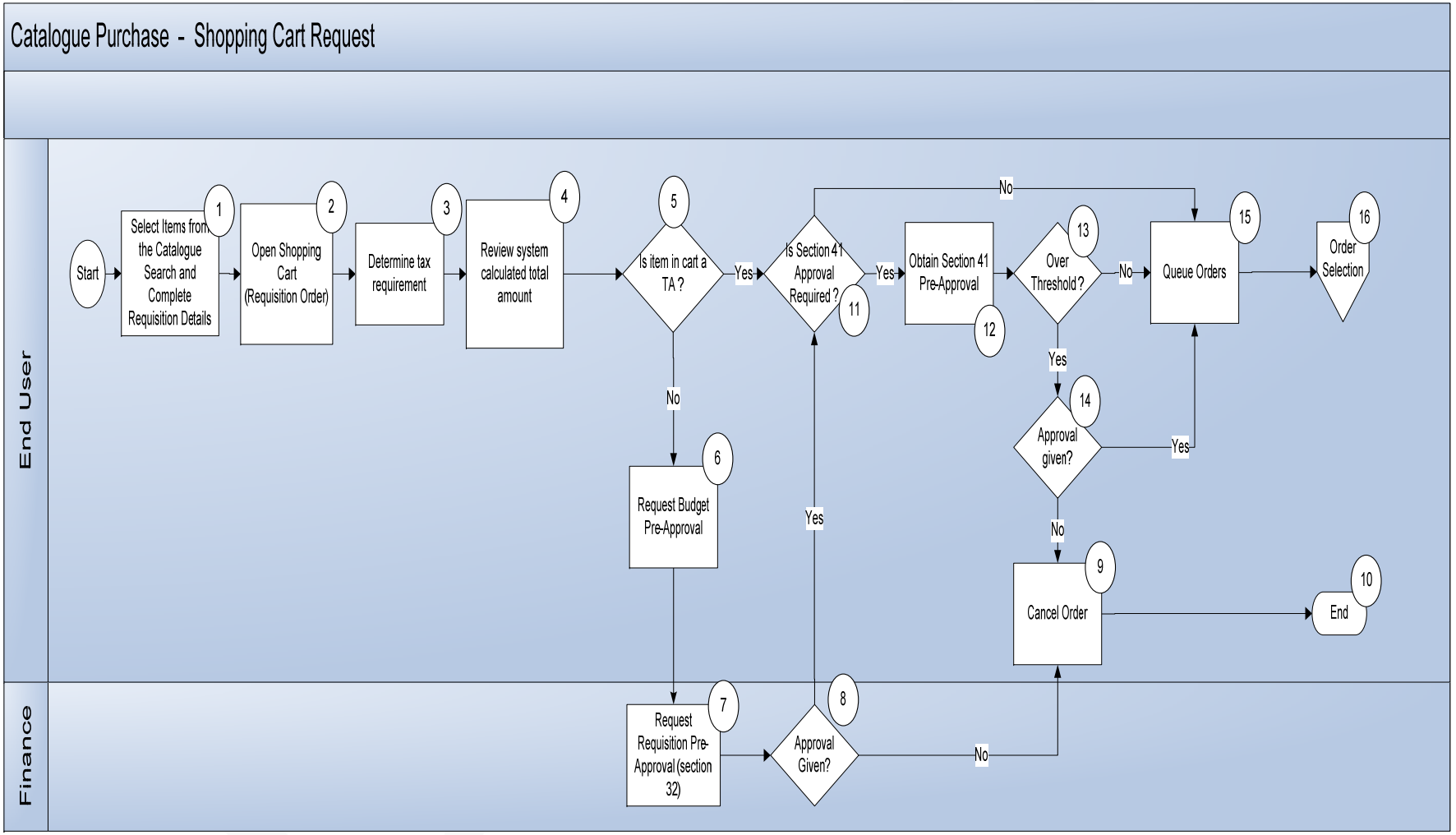


Figure 5 - Level 2 Shopping Cart Request Business Process Model

Process Description

Shopping Cart Request	
Summary Description	The purpose of the Shopping Cart Request process is to select goods and/or services to be purchased from the Catalogue. This sub process ensures that (1) the Requisition Order is either cancelled or sent to Order Selection and (2) Budget Pre-Approval is given before orders can be queued/sent to Order Selection A shopping cart request may contain one or more items of one or more types. One of which could be a Task Authorization (TA) from one or more catalogues. The only exception in the process is the need for a section 32 or 41 pre-approval when an item in the cart is not a TA, regardless of the type of items.
Process Narrative ***Actors:*** • ***End-user with authority to issue an order. The End User is either the Proxy Requester or Client Requester***	The following process flow narrative pertains to Figure 5: 1. The End User will have the ability to select items from the Catalogue. The End User will be able to search and complete the requisition order details. A search is a generic way of finding desired good(s) and/or service(s) in the catalogue. The search is categorically driven (e.g. goods or services). An example among many of how the End User will search is seen directly below: • Select 'goods' o Select 'furniture' ▪ Select 'chair' • Select 'lazy-boy office chair' 2. When items are selected, they are placed in the Shopping Cart (requisition order). A shopping cart request is done for one catalogue. If goods or services are selected from more than one catalogue, multiple requests are made. This will become multiple orders with multiple supplier shopping cart requests. The user may create a Shopping Cart request on behalf of another user or client department. If this occurs then the proxy requester must identify the client requester and the procurement financial codes. 3. A calculation is required taking into account the item price(s). There are two possible approaches here. Firstly, the End User can enter and estimate taxes. Secondly, the system will provide a generated tax based on the service/good delivery location. Please note this is an estimated tax for the order (e.g. sack estimation). Most of the time, the Supplier will be establishing the tax value 4. The End User will review the system calculated total value. 5. The question is asked whether the item(s) in the Shopping Cart is/are a TA. 6. If not, the End User requests budget approval 7. After the Budget Pre-Approval, the Request for Section 32 Pre-Approval is completed. The user will request a Section 32 pre-approval from Finance and indicate to EPS that the purchase can be made. The funds need to be committed in the financial system. The accounting codes are in the catalogue. When finance indicates the funds are available the supplier shopping cart request is sent to the suppliers with delivery information and complete shopping cart details. The user may attach supporting documents for the supplier. 8. Afterwards, the question is asked whether approval is given.

	9. If approval is not given, the order is cancelled and the End User is then notified of the cancellation. 10. The process ends. 11. If approval is given, the question is asked whether Section 41 approval is required. 12. If Section 41 approval is required, the End User will request a budget pre-approval to check the total amount against the departmental budget. 13. The question is asked whether or not the total dollar value of the order is over the threshold. 14. If the total dollar value of the order is not over the threshold or if Section 41 approval is not required, the order(s) may be queued. Queuing orders is the process of grouping multiple shopping carts requests from one or more users into one shopping cart request based on configurable catalogue business rules (e.g. geographic location, deliverable date, lead time, client department, tiered pricing). 15. After the queuing is complete, the process proceeds to selection of a supplier. 16. If the order(s) is/are over the threshold, approval is required before continuing. If approval is given, the End User will queue the order(s). If approval is not given, the order is cancelled. In either case the user will be notified.

Input	Description
Items (goods and/or services)	Items selected from the catalogue
Section 32 commitment	This approval will come from FINANCE indicating that the procurement can proceed. The money is available
Approval is received	Approval from the contracting officer or senior management when a purchase exceeds the financial threshold for the user
Section 41 commitment	This is approval coming from the CO to indicate that an order can be issued.

Output	Description

Shopping Cart (Requisition Order)	A Shopping Cart (Requisition Order) is created with goods and /or services
Approval Request	An e-mail request has been sent to the approver when spending exceeds commitment amount or, Requester's authorized amount.
Financial codes for commitment	A Section 32 Commitment is made to SAP (Finance Accounting ERP) for budget confirmation.

Business Rules

The Shopping Cart Request business process is governed by the following rules:

1. Each request contains goods/services from one catalogue only.
2. A proxy requester has authorization to procure goods on behalf of another client or user if their user profile permits.
3. The catalogue search for specified items is done within End-User's region. Only goods & services for the same region as the requester are shown.
4. A shopping cart request can be amended or canceled.
5. The approver is based on delegation of authority.
6. The order may be queued based on good or service and delivery date.

d. Order Selection

Process Model

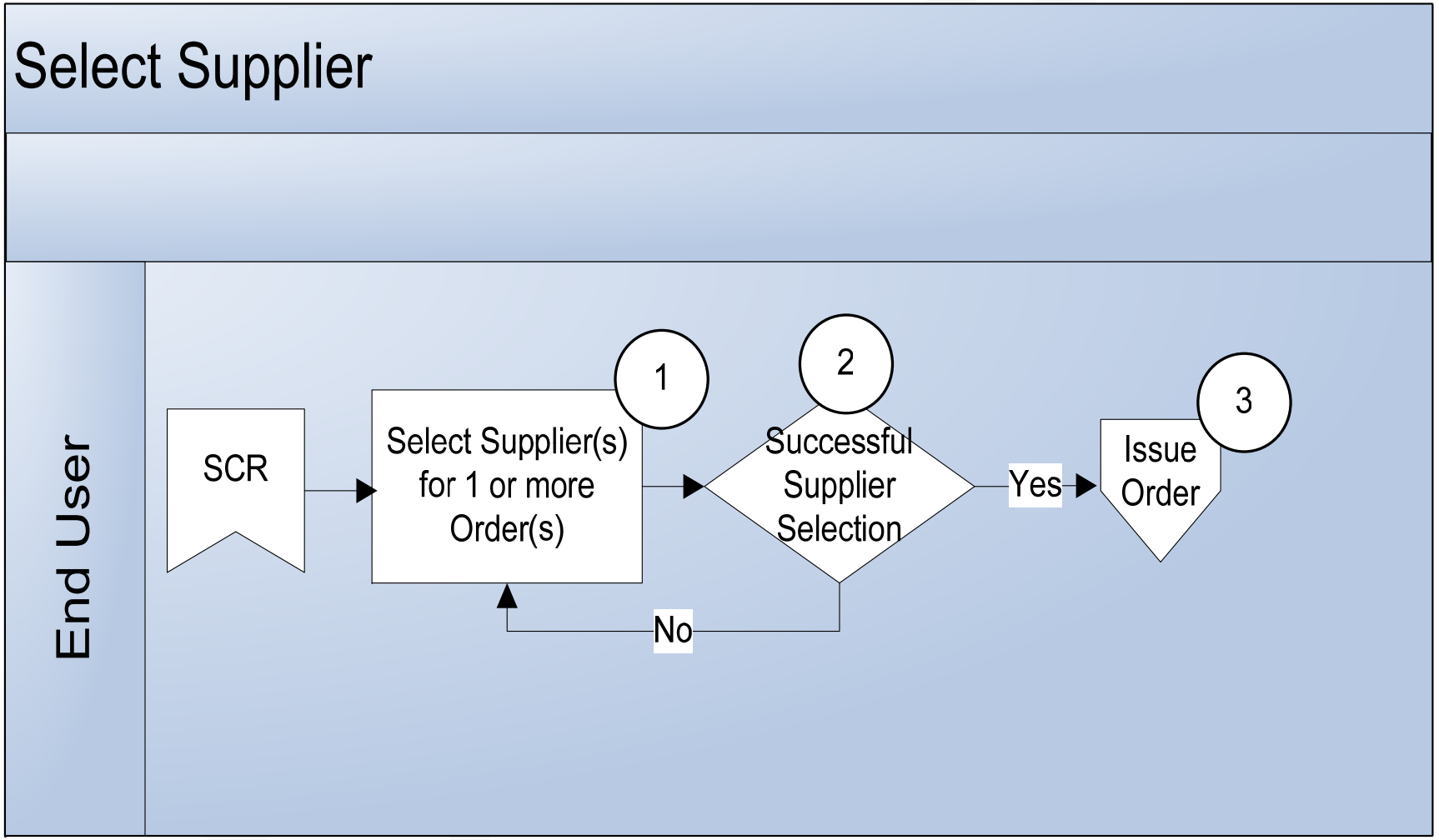


Figure 6 - Level 2 Order Selection Business Process Model

Process Description

Order Selection	
Summary Description	This process involves selection of a supplier for an order
Process Narrative ***Actors:*** • ***End-user with authority to amend an order*** • ***The End User is either the Proxy Requester or Client Requester***	The following process flow narrative pertains to Figure 6: 1. A supplier is selected for one or more orders 2. Upon return from selecting a supplier, confirmation is obtained regarding the selection being successful. If it is not, the process returns to repeat the selection process. 3. If supplier selection is successful, the process proceeds to Issue Order.

Input	Description
An Order (Purchase Order)	An order in the shopping cart
Output	**Description**
Successful Supplier	A Supplier is selected for an order

Business Rules

The Select the Supplier business process is governed by the following rules:

1. As a pre-condition, an Order must have been created in the shopping cart
2. A validation check is done after the Supplier(s) are selected. This is to confirm that the Supplier is still able to fulfill the order (e.g. lack of resources, supplier bankruptcy).

e. Issue Order

Process Model

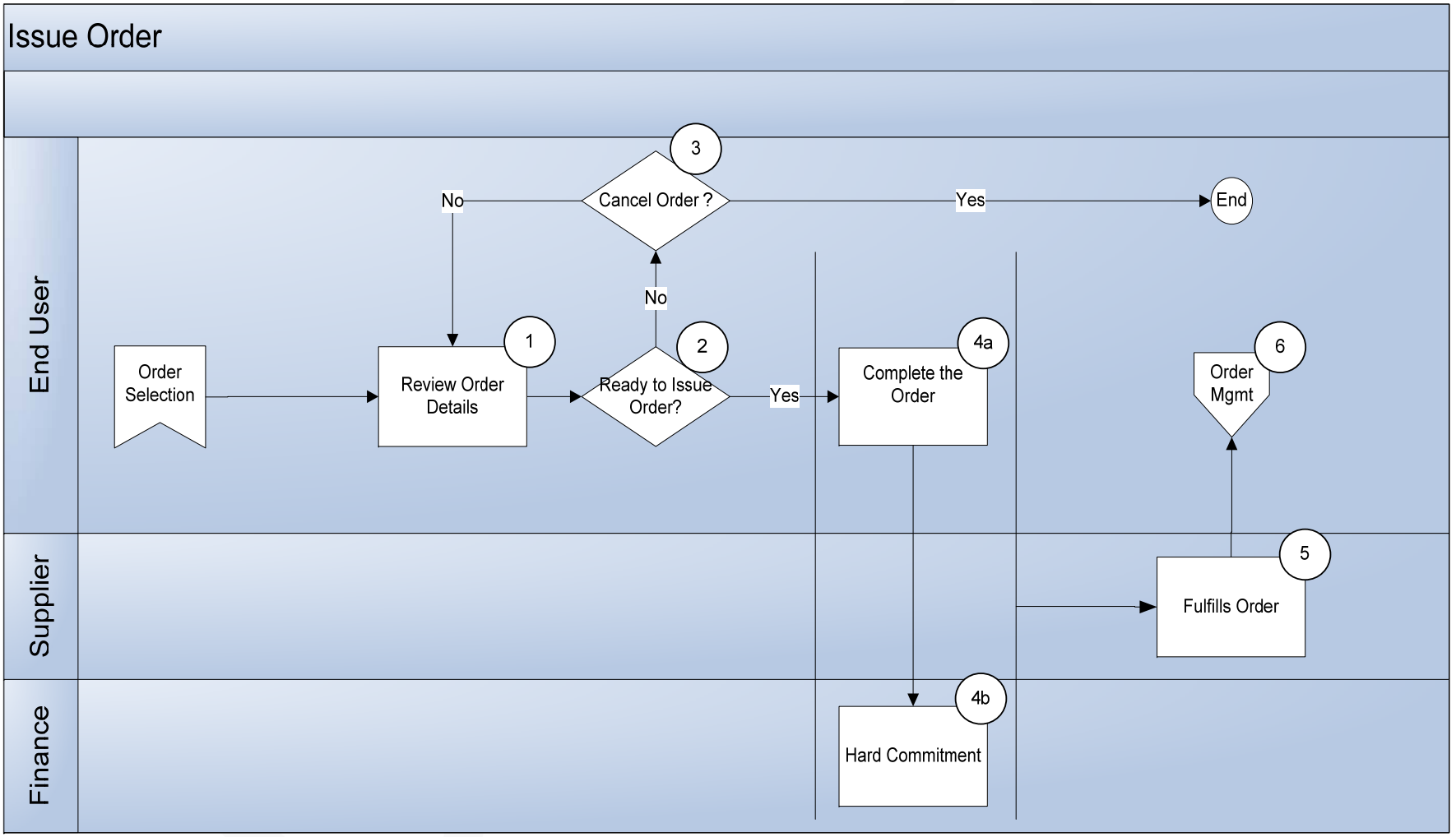


Figure 7 - Level 2 Issue Order Business Process Model

Process Description

Issue Order	
Summary Description	This process involves reviewing, completing and fulfilling the order. The sub process ensures that: • The End User and Finance collaboration to complete the order • The Supplier fulfills the order
Process Narrative ***Actors:*** • ***End-user with authority to issue an order*** • ***The End User is either the Proxy Requester or Client Requester*** • ***Pre-qualified supplier*** • ***Qualified Approver***	The following process flow narrative pertains to Figure 7: A Shopping Cart Request will exist and the order changes from a requisition order to a purchase order. 1. The End User will review the order details (e.g. quantity, delivery location/time, item description, financial coding). 2. The End User will be asked whether they are ready to issue the order. This validation step is required before the order can be placed. 3. If the End User decides to cancel the order they can cancel the shopping cart request and the process ends. If the End User decides not to cancel the order, they return to continue reviewing the order details. 4. If the End User proceeds with the order the following steps are done simultaneously: a. The order is completed. b. A hard commitment is sent to Finance. When an order is issued to Finance, it can be assigned to different fiscal years (e.g. 200k for year 1 and 100k for year 2 which accumulates to a total order value of 300k) 5. A copy of the order is sent to the Supplier to process. The Supplier then fulfills the order. 6. The process proceeds to Order Management.

Input	Description
Commitment confirmation	Finance (SAP) will return the confirmation of a hard commitment for the order.
Shopping Cart Request	From the shopping cart request, the user will determine how to split the commodity requirements.
Output	**Description**
Purchase Order	An Order is created and sent to Finance (SAP) for a hard commitment.
Purchase Order Issued	The PO is sent to the supplier for signing and processing.

Hard commitment request	A hard commitment request is sent to Finance (SAP) for confirmation to issue the order to the supplier.

Business Rules

The Issue Order business process is governed by the following rules:

1. As a pre-condition, a Shopping Cart (requisition order) must exist

f. Order Management

Process Model

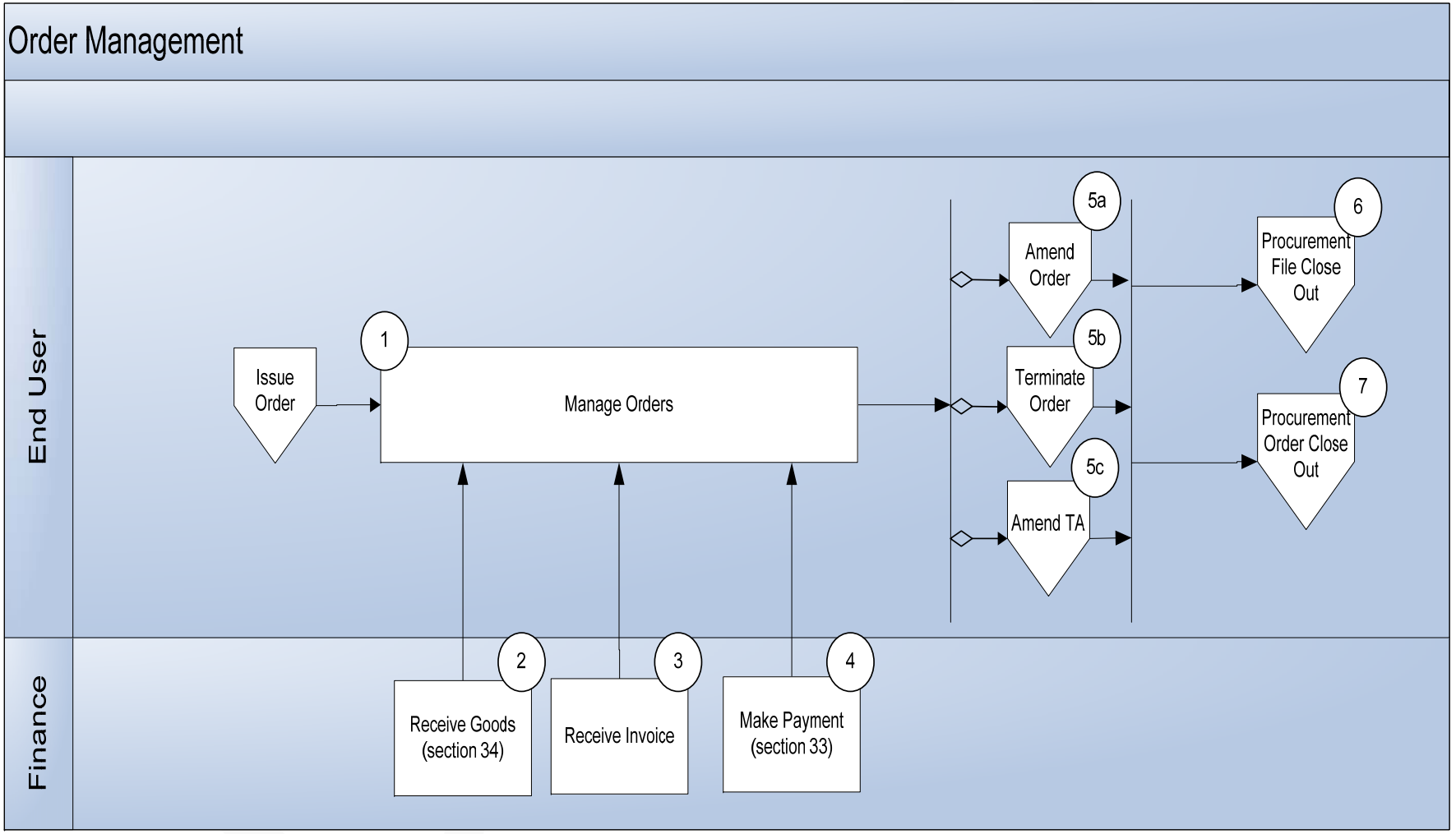


Figure 8 - Level 2 Order Management Business Process Model

Process Description

Order Management	
Summary Description	The purpose of this Order Management process is manage the order until it is amended, terminated or closed.
Process Narrative ***Actors:*** • ***End-user with authority to amend an order*** • ***The End User is either the Proxy Requester or Client Requester***	The following process flow narrative pertains to Figure 8: 1. In order management, there are three activities that are managed by Finance using SAP. These are Receiving Goods, Receiving the Invoice and Making a Payment (Section 33). 2. Receiving Goods involves the receipt of goods by the End User from the Supplier 3. Receiving the Invoice involves the End User receiving the invoice from the supplier 4. Making a Payment (Section 33) involves the End User paying the Supplier invoice. 5. The process will continue to one of the following: a. Amend the Order b. Amend the Task Authorization c. Terminate an Order. 6. The End User then initiates the process to close the Procurement File or: 7. Close the Procurement Order as and when required.

Input	Description
An Order (Purchase Order)	An order has been issued. An amendment may also have occurred.
Notification that goods are received	Coming from Finance ERP
Notification that invoice received	Coming from Finance ERP
Notification that payment is made	Coming from Finance ERP
Trigger to Close Order	An order close date or end user invoked
Output	**Description**
Go to terminate order	End user decision from order management
Go to amend order	End user decision from order management

Business Rules

The Order Management business process is governed by the following rules:

1. As a pre-condition, an Order must have been issued and a hard commitment made.

g. Order Close Out

Process Model

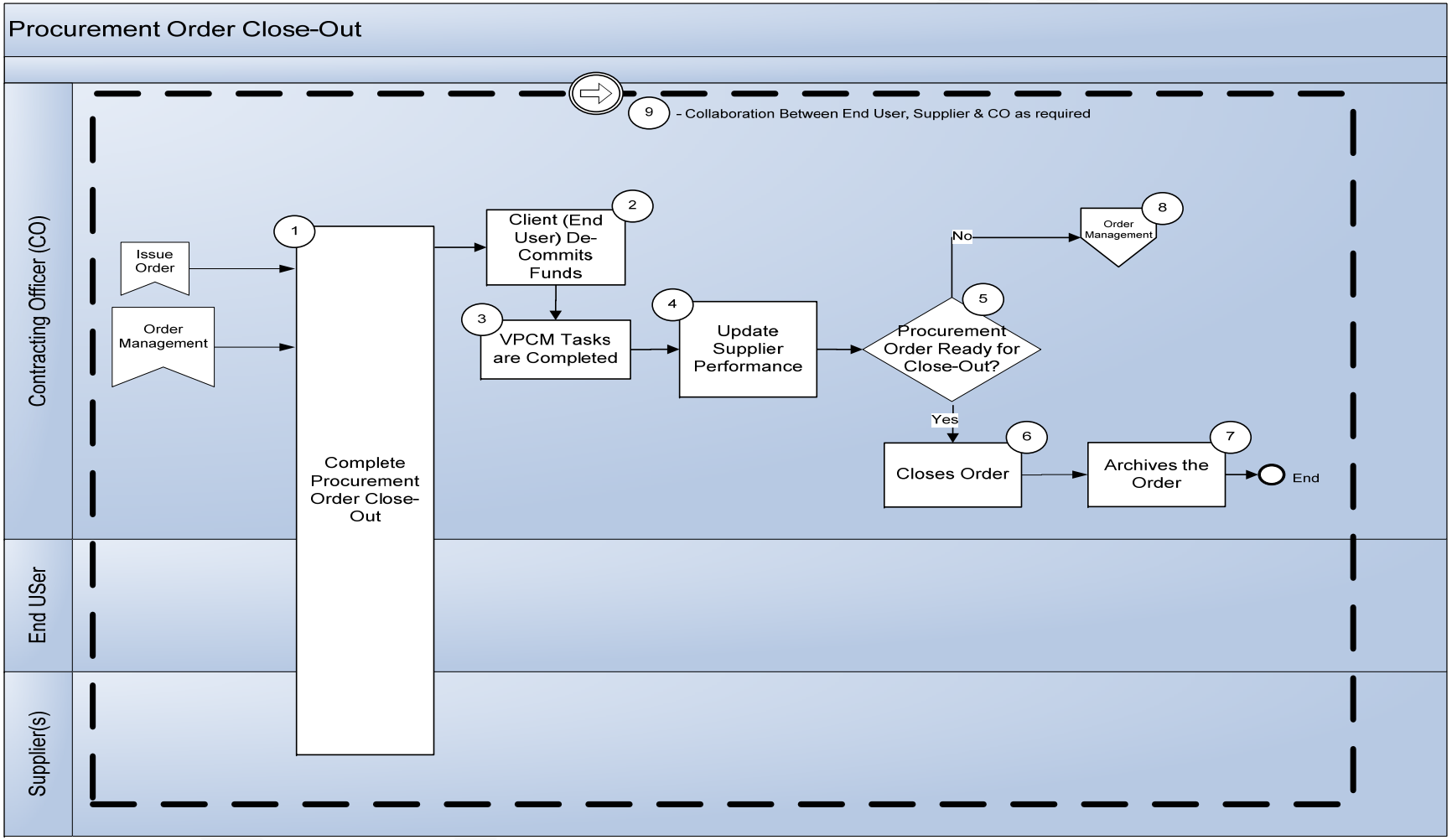


Figure 9 - Level 2 Order Close-Out Business Process Model

Process Description

Order Close Out	
Summary Description	The purpose of this Procurement Order Close Out process is to complete and close the order. This sub-process includes steps to ensure that, • contract deliverables were delivered • all issues are resolved • all invoices are paid • supplier performance evaluation is conducted and • the order is archived according to records management policy
Process Narrative ***Actors:*** • ***End-user with authority to amend an order*** • ***The End User is either the Proxy Requester or Client Requester***	The following process flow narrative pertains to Figure 9 : 1. The CO along with the End User, can complete the order close-out by: i. Determining when the final Supplier performance evaluation is conducted ii. Listing all invoices/progress claims that are paid iii. Determining when all contractual deliveries are completed iv. Ensuring that there are no unresolved issues v. Ensuring that all required forms were completed vi. Ensuring that the Contract is Complete 2. The CO also ensures that de-committing of funds is completed by the Client (End User) if there are financial commitments that remain 3. The CO also ensures that all tasks re: Suppliers Performance Corrective Measures (VPCM) are completed 4. The CO ensures that supplier performance is updated 5. The CO confirms that the order can be closed and archived When the order **is** ready to be closed: 6. Using the EPS solution, the CO closes the order 7. Using the EPS solution, the CO archives the order information When the order is **not** ready to be closed: 8. The CO continues to perform Order Management 9. Collaboration occurs between the CO, Supplier and Client (End User) as required throughout the process.

Input	Description
Completed Order (Purchase Order)	An order has been completed
Output	**Description**
Closed & Archived Order	Order that has been closed & archived

Business Rules

The Procurement Order Close-Out business process is governed by the following rules:

1. A pre-condition is an Order must have been completed.

7.2. Level 3 Business Process Models and Descriptions

a. Amend the Order/Catalogue

Process Model

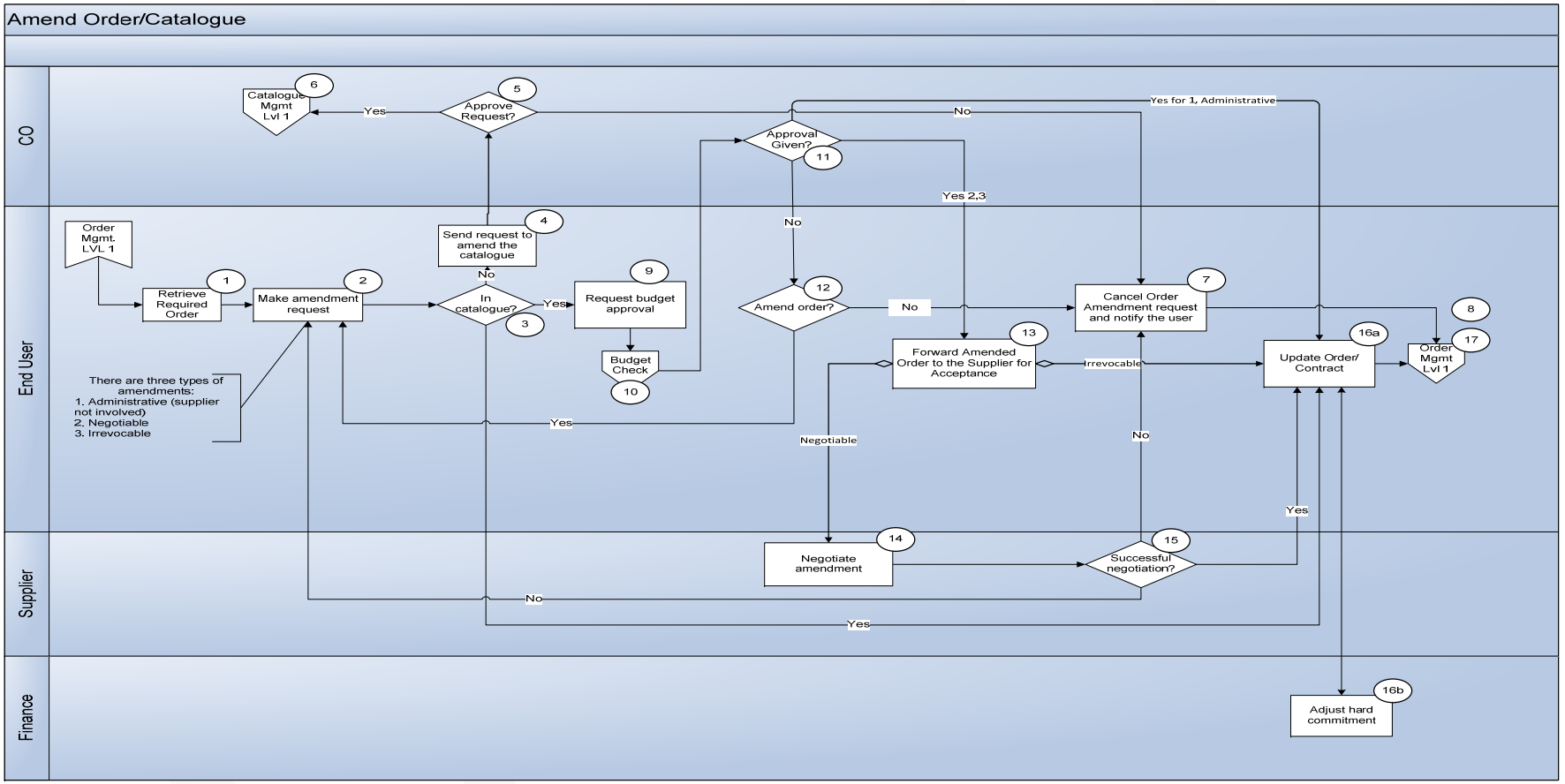


Figure 10 - Level 3 Amend Order Business Process Model

Process Description

Amend an Order/Catalogue	
Summary Description	The purpose of the Amend the Order sub-process is to seek approval to amend a contract/standing offer/supply arrangement. The amendment approval authority required will determine the document to be used.
Process Narrative ***Actors:*** • ***End-user with authority to amend an order*** • ***The End User is either the Proxy Requester or Client Requester*** • ***Pre-qualified supplier*** • ***Qualified Approver***	The following process flow narrative pertains to Figure 10: 1. The End user will make a search to retrieve the order by typing the order number. 2. The End User will create an amendment request. There are three types of amendment requests: a. **Administrative** (supplier is not involved) occurs when changes are administrative (e.g. name change of technical authority) It can also occur when End User is transferring money in contract per period of time without changing the contract value. There is no Section 34 and 41 involved. Therefore, the order is directly updated without seeking these approvals. b. **Negotiable** (supplier is involved) occurs when changes are negotiated (e.g. extending time or dollar value of an order) c. **Irrevocable** (e.g. excising option period of an order where the supplier has to accept the changes) 3. The End User will determine if the item(s) are in the catalogue. 4. If the item(s) in the amendment request are not in the catalogue, the End User requests the CO to amend the catalogue and add the item(s). 5. The CO will approve or reject the amendment request. 6. If the CO accepts the request, the item(s) will be added to Catalogue. This step is conducted in the Catalogue Management Process. 7. If the CO rejects the amendment request, it will be cancelled. 8. If cancelled, the process returns to Order Mgmt. 9. If the item is in the catalogue, the End User requests Budget Approval. 10. After the Budget Check is complete, the CO has to provide further Section 41 approval. 11. If CO approval is not given, the End User will decide to continue with the Amendment Request. If they decide to continue, the Amendment Request is updated. If not, the Amendment Request is cancelled. 12. If CO approval is given for types 2 negotiable and 3 irrevocable, the process proceeds to step 14. If CO approval is given for type 1 administrative, the process proceeds to step 16a. 13. For type 2 negotiable, the End User will forward the amendment request to the supplier for acceptance. For type 3 irrevocable the order will be updated and sent to the Order Mgmt Process.

	14. If the amendment request is negotiable, negotiation will occur with the supplier to finalize the amendment request. 15. If the negotiation is successful between the End User and Supplier the order will be updated and sent to the Order Mgmt Process. If the negotiations are not successful, there are two options. Option 1 is the Amendment Request is cancelled at step 7 or option 2 new changes are made to the Amendment Request at step 2. 16. The following two steps are conducted simultaneously: a. the order contract is updated. b. Finance adjusts the hard commitment. 17. The process returns to the Order Management process

Input	Description
An Order (Purchase Order)	An order has been issued. An amendment may also have occurred.
Approval	Approval is required to amend an existing Order. (refer to Section 18 – Governance)
Output	**Description**
Notification to supplier	Notification of Amendment is sent to the Supplier for clarifications and negotiations until an agreement is made.
Amended Order	The original Order is amended.
Financial update sent to Finance (SAP)	The change to the price is sent to finance to change the commitment.

Business Rules

The Amend the Order/Catalogue business process is governed by the following rules:

1. There are three types of amendments as follows: negotiable, administrative, and irrevocable
2. If the type is negotiable or irrevocable, the supplier will be involved with the amendment.
3. As a pre-condition, an Order has been issued and a hard commitment is made

b. Amend Task Authorization (TA)

Process Model

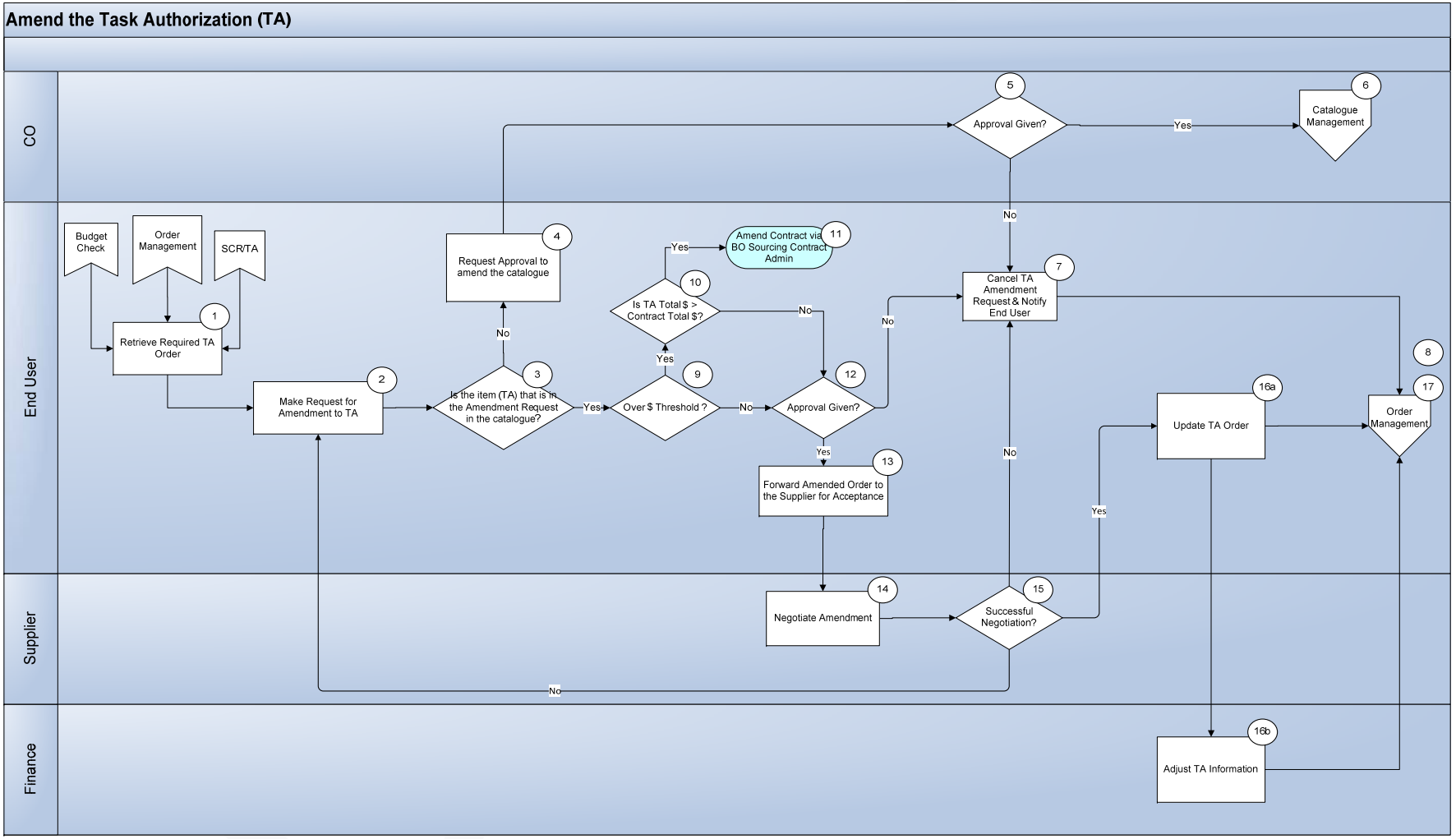


Figure 11 - Level 3 Amend TA Business Process Model

Process Description

Amend a Task Authorization (TA)	
Summary Description	The purpose of the Amend a Task Authorization sub-process is to amend or cancel a TA. A contract with Task Authorizations (TAs) is a method of supply for services under which all of the work or a portion of the work will be performed on an "as and when requested basis" through predetermined conditions. These conditions include an administrative process involving task authorizations. A TA is a structured administrative tool enabling PWGSC and/or a client to authorize work for a contractor on an "as and when requested" basis in accordance with the conditions of the contract. In some circumstances, a TA will have to be amended (e.g. time, money, and cancellation).
Process Narrative ***Actors:*** • ***End-user with authority to amend an order*** • ***The End User is either the Proxy Requester or Client Requester*** • ***Pre-qualified supplier*** • ***Qualified Approver***	The following process flow narrative pertains to Figure 11: 1. The End User searches to retrieve TA information 2. The End User creates an amendment request 3. The End User determines if the item(s) in the amendment request are in the catalogue 4. If the item(s) in the amendment request are not in the catalogue, the End User requests the CO to add the item. 5. The CO will approve or reject the amendment request. 6. If the CO accepts, the item will be added to Catalogue. This step is conducted in the Catalogue Management Process.. 7. If approval is not given, the TA Amendment Request is cancelled and the End User is notified. 8. After cancellation, the process returns to Order Mgmt. 9. If the item in the TA Amendment Request is in the catalogue, the question is asked whether or not the request is over the dollar threshold. 10. If the request is over the threshold, the question is asked whether or not the TA total dollar value is greater or less than the contact total dollar value. 11. If greater, the contract is amended in the Sourcing Contract Administration process. 12. If the request is less than the contract total dollar value, approval is required by the CO. Similarly, if the TA Amendment Request is not over the threshold, the same CO approval is required to proceed. If approval is not given, the TA Amendment Request is cancelled and the End User is notified. 13. If the Amendment Request is approved, the TA is forwarded to the Supplier. 14. The Supplier can then negotiate the amendment. 15. If negotiations are not successful, the TA Amendment Request is cancelled, with the End User being notified or a new amendment is requested.

	16. If the negotiations are successful, the following two steps are conducted at the same time and then sent to Order Management: a. The TA Order is updated. b. Finance adjusts the TA information. 17. The process returns to the Order Management process

Input	Description
An Order (Purchase Order)	An order has been issued. An amendment may also have occurred.
Approval	Approval is required to amend an existing Order. (refer to Section 18 – Governance)
Output	**Description**
Notification to supplier	Notification of Amendment is sent to the Supplier for clarifications and negotiations until an agreement is made.
Amended Order	The original Order is amended.
Financial update sent to Finance (SAP)	The change to the price is sent to finance to change the commitment.

Business Rules

The Amend the Task Authorization business process is governed by the following rules:

1. There are three types of amendments as follows: negotiable, administrative, and irrevocable
2. If the type is negotiable or irrevocable, the supplier will be involved with the amendment.
3. As a pre-condition, an Order has been issued and a hard commitment is made

c. Terminate the Order

Process Model

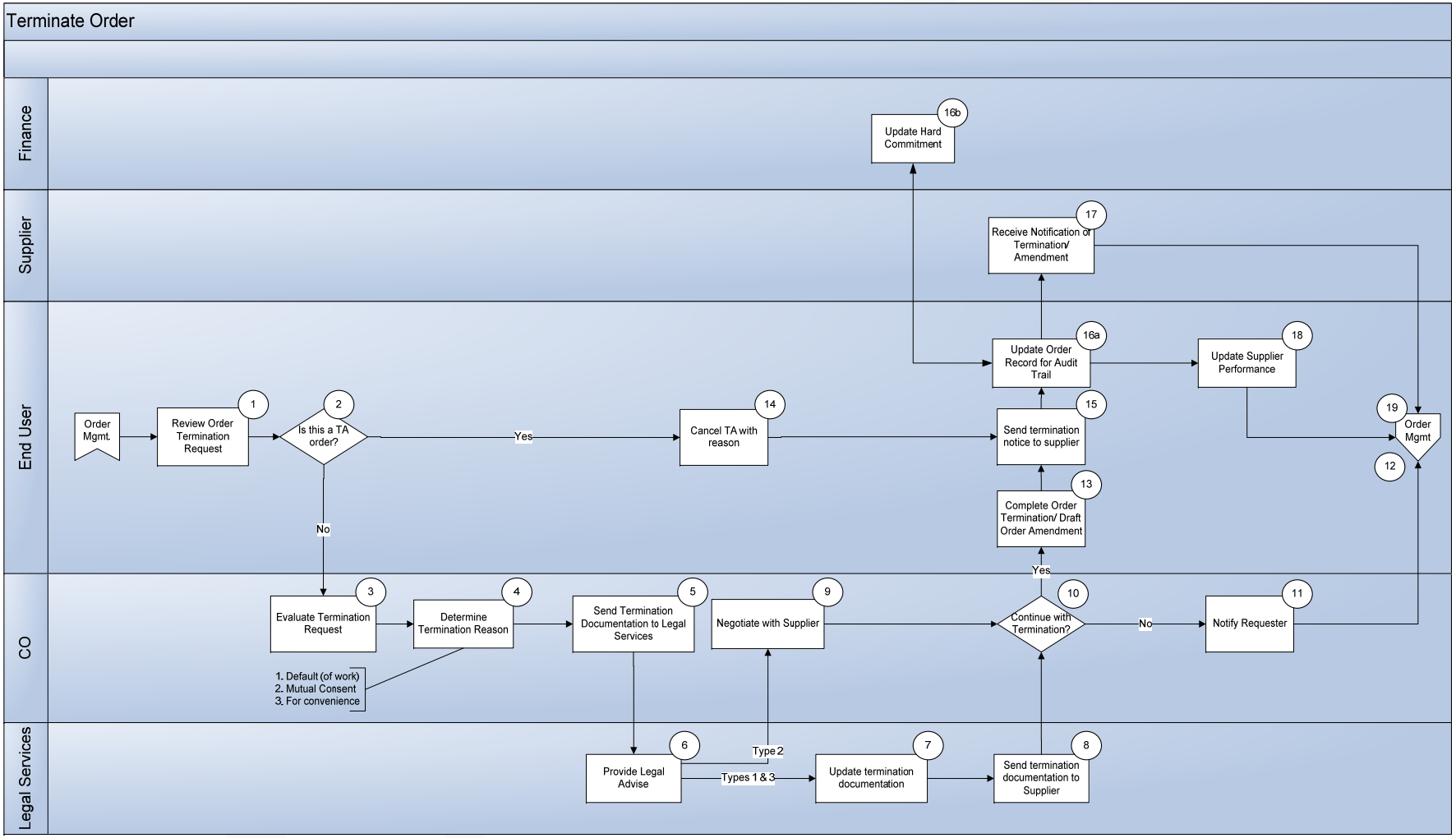


Figure 12 - Level 3 Terminate Order Business Process Model

Process Description

Terminating an Order	
Process Description	The purpose of the Terminating an Order sub-process is to determine if the Order will be terminated. This sub-process includes steps for: • Distinguishing whether the order is a TA • Determining three types of termination reasons • Receiving information from Legal Services, Finance, and the CO in order to determine if the order will be terminated
Process Narrative ***Actors:*** • ***End-user with authority to amend an order*** • ***The End User is either the Proxy Requester or Client Requester*** • ***Pre-qualified supplier*** • ***Qualified Approver***	The following process flow narrative pertains to Figure 12: 1. The End User will review the order termination request. 2. This review includes an examination of whether the order termination request includes a TA. 3. If the termination request is a TA Order, the CO will evaluate the termination request. 4. From here, the CO will determine the termination reason among a choice of three. These reasons include: a. **Default (of work)** – The decision to terminate a contract for default should be made only after all other possible solutions have been explored. In all cases, the advice of Legal Services must be obtained at an early stage, to ensure that any proposed action will not prejudice Canada's legal position and that the termination is legally enforceable. b. **Mutual Consent** – On rare occasions both parties may agree to termination without claims or penalties, usually where the client has requested full or partial termination of a contract, the contractor has incurred minor or no expenses and is willing to not pursue a claim, and the matter may be settled at no cost to Canada. Termination by mutual consent does not apply when it is in Canada's interest to issue a termination for default or when the contractor claims additional costs following the reduction or cancellation of all or a portion of the contract. c. **Convenience** – Canada may terminate a contract for convenience in accordance with the termination for convenience provision of the general conditions applicable to the contract. This may be due to curtailment of funds, discontinuation of a government program, or other circumstances, which make the procurement of the good or service unnecessary. To protect the integrity of the bid solicitation process, Canada may also terminate a contract for convenience, if it is determined that it has been

	mistakenly awarded to other than the lowest-responsive bidder. 5. The CO will send the termination documentation to Legal Services. 6. Legal Services will provide Legal Advice on the termination documentation. 7. If the termination reason is either Default (of work) or Convenience, Legal Services will then update the termination documentation. 8. Legal Services will send termination documentation to the supplier. 9. After Legal Advice has been provided, if the termination reason is mutual consent, the CO will negotiate with the supplier. 10. All termination reasons will need the CO to decide to continue or end the termination request. 11. If the CO does not continue the termination request, the requester is notified. 12. The process returns to Order Mgmt. 13. If the Termination is continued by the CO, the End User will complete the order termination and will draft an order amendment. 14. If the termination request is a TA order, the TA is cancelled with a reason. 15. The End User will send the termination notice to the supplier. This occurs when either step occur: the order termination is completed or if the TA order is cancelled. 16. The following steps occur simultaneously: a. The End User updates the Order Record for Audit Purposes b. Finance updates the Hard Commitment and exchanges this information with the End User. 17. The Supplier receives notification of the termination/amendment. 18. The End User updates the Suppliers performance. 19. The process returns to Order Management.

Input	Description
An Order (Purchase Order)	An order has been issued. An amendment may also have occurred.
Output	**Description**
Notification to Legal Services	Notification of an Order termination has been sent to Legal Services for processing.
Terminated Order	The Order is terminated.
Financial update sent to Finance (SAP)	Funds are de-committed.

Business Rules

The Terminating an Order business process is governed by the following rules:

1. There are three types of amendments as follows: negotiable, administrative, and irrevocable.

2. Only the CO can determine the reason.
3. 'Mutual Consent' will happen between CO and Supplier (negotiating).
4. The part of this process that involves Legal Services is a legal process and are not part of EPS. Only recording of the outcome of the legal process will be required in EPS for audit trail purposes
5. As a pre-condition, an Order has been issued and a hard commitment is made

7.3. Level 4 Draft Business Process Models and Descriptions

a. Budget Check

Process Model

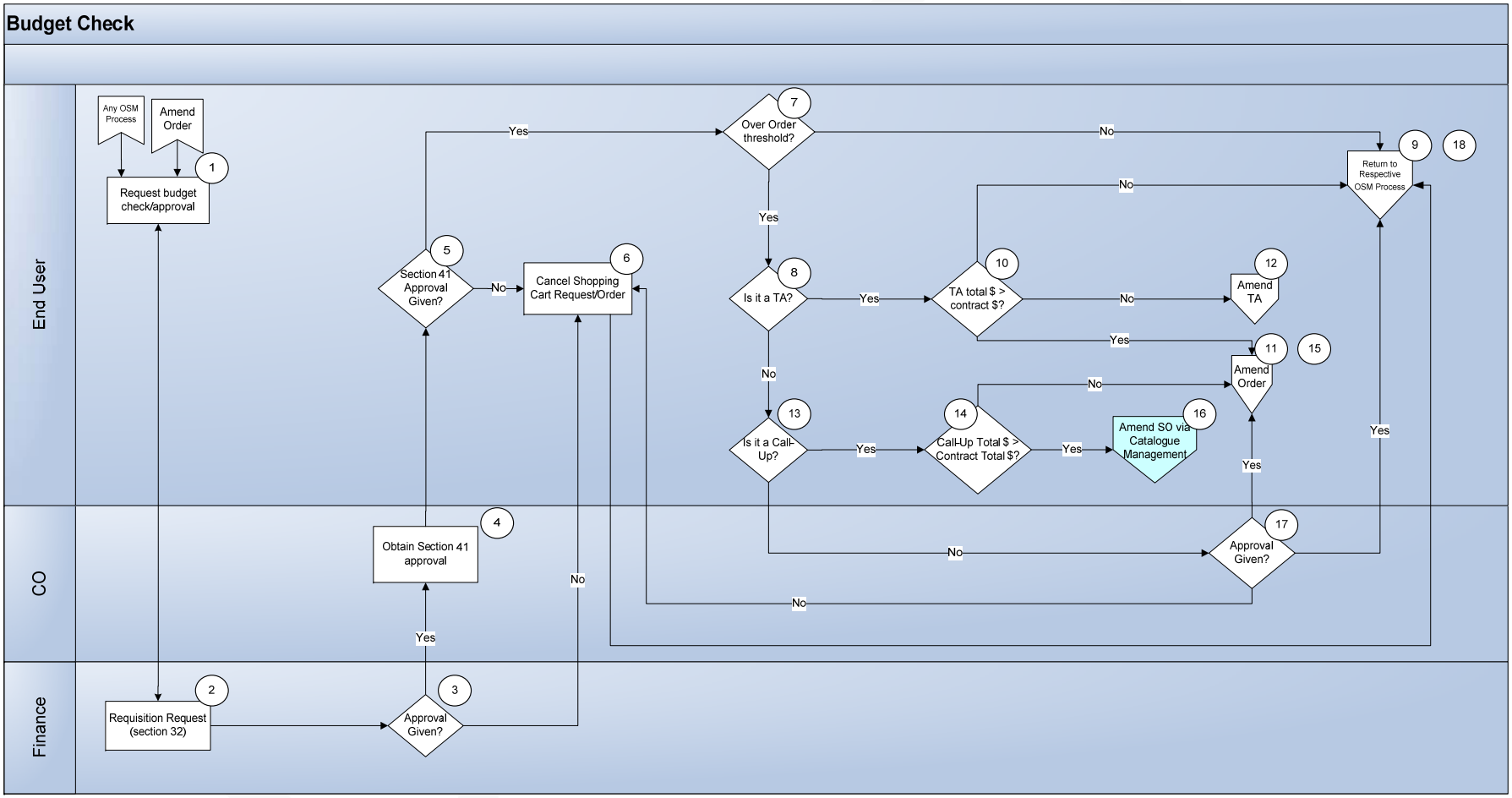


Figure 13 - Level 4 Budget Check Business Process Model

Process Description

Budget Check	
Process Description	The purpose of the Budget Check sub-process is to determine if the SCR/Order is approved by Finance (SAP) for the funds required to complete the order. This sub-process includes steps for: • Obtaining Section 41 and 32 Approval • Cancelling an Order if the funds required are not approved • Distinguishing whether the order is a TA or a Call-Up
Process Narrative ***Actors:*** • ***End-user with authority to issue an order.*** • ***The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer***	The following process flow narrative pertains to Figure 13: 1. The Requisition Request (Section 32) will be created by Finance (SAP) 2. The section 32 request requires approval by Finance (SAP). 3. If approval is given, the Requisition Request will be sent to the CO for Section 41 approval. If approval is not given, the Shopping Cart Request/Order is cancelled after which the process returns to Order Selection (OS). 4. It is requested of the CO to approve the section 41. 5. If the End User obtains Section 41 approval, the total dollar value before taxes of the request is checked to determine if the value is over the threshold. 6. If the End User does not obtain Section 41 approval, the Shopping Cart Request/Order is cancelled and the process returns to the respective Order Selection (OS). 7. If Section 41 approval is given to the End User, it is determined whether the Shopping Cart Request/Order is over the threshold. 8. If the Shopping Cart Request/Order is over the threshold, the question is asked whether it is a TA. 9. If the Shopping Cart Request/Order is not over the threshold, the process returns to the respective Order Selection (OS). 10. If the Shopping Cart Request/Order is a TA, it is evaluated whether or not the TA total dollar value is greater than the Contract total dollar value. 11. If the TA dollar value is greater than the total contract value, the order must be amended. If the TA dollar value is less than the total contract value there are two options. The first option is the process returns to the respective Order Selection (OS). 12. If the TA dollar value is less than the total contract value, the second option is to amend the TA. 13. If the Shopping Cart Request/Order is not a TA, the question is asked whether it is a Call-Up. 14. If yes, the Call-Up's total dollar value is compared to the contract total dollar value. 15. If the Call-Up's total dollar value is less than the contract total dollar value, the process proceeds to amend the Order.

	16. If the Call-Up's total dollar value is greater than the contract total dollar value, the Standing Offer is amended via Catalogue Management. 17. If the Shopping Cart Request/Order is not a Call-Up, approval is needed by the CO to continue. If the CO does not approve, the Shopping Cart Request/Order is cancelled, and the process returns to the respective Order Selection (OS). 18. If the CO approves the Budget Check, the process returns to the respective Order Selection (OS).

Input	Description
Shopping Cart Request	This will come from the Order Selection (OS) process.
Output	**Description**
Approval notification	The CO will notify the end user when Section 32, Section 41 and over spend request. The notification will specify whether the request was approved or not.
Order Cancellation	If approval is not received then the order is cancelled.

Business Rules

The Budget Check business process is governed by the following rules:

1. Section 32 Budget
2. Section 41 Amount (contract admin)
3. The User threshold
4. Department Budget
5. PWGSC Budget
6. Financial Delegation
7. As a pre-condition, a shopping cart request exists

8. SOURCING PROCUREMENT

8.1. Level 2 Business Process Models and Descriptions

a. Requisition Management

Process Model

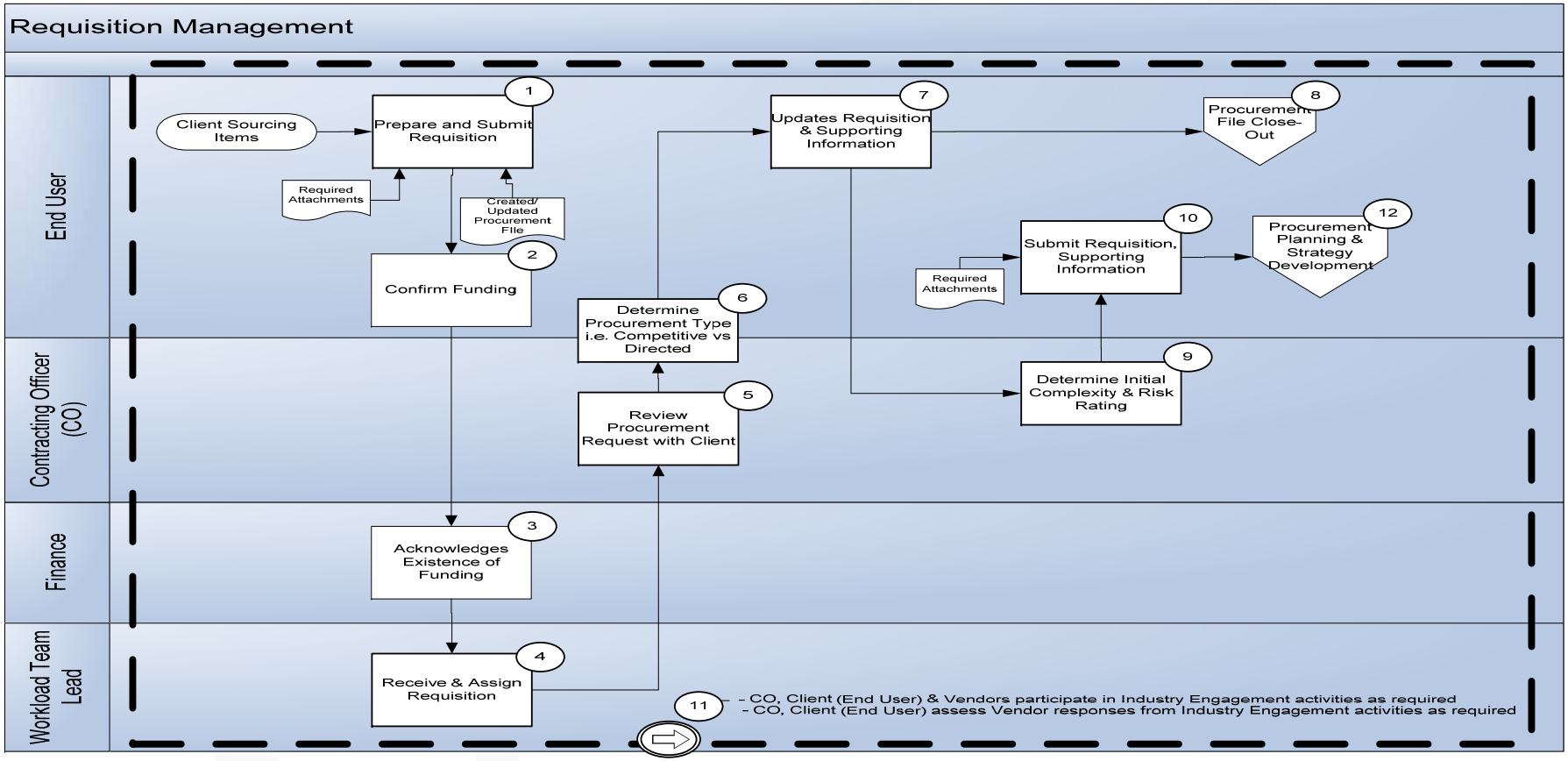


Figure 14 - Level 2 Requisition Management Business Process Model

Process Description

Requisition Management	
Summary Description	The purpose of the Requisition Management process is to determine the requirement for procurement of goods/services as well as general requisition management. This sub-process includes steps for: • Clients (End User) to define procurement requirements in their entirety • Clients (End User) to obtain project approval • Client (End User) to submit requisition(s) to PWGSC/client dept • Clients (End Users) submits a request to certify availability of funds • PWGSC/client dept to coach and mentor Clients (End User) in determining the best way forward, identify special requirements (e.g. green procurement, security, progress reports, special packaging, transportation, bonding) that suppliers may need to address in their bids. • Clients (End User) and PWGSC/client dept to engage external expertise to assist with the definition of the requirement • Clients (End User) to justify non-competitive procurement or sole source when required • Clients (End User) & contracting authorities to determine procurement type as being competitive versus non-competitive
Process Narrative ***Actors:*** • ***End-user. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Workload Team Lead***	The following process flow narrative pertains to Figure 14: 1. When the Client (End User) requires CO involvement in their sourcing procurement, or when they cannot purchase their desired items via catalogues, after receiving the proper approvals, they prepare and submit, via EPS, a requisition. 2. The Client (End User) confirms the existence of funding for the purchase with the Finance (SAP) system. 3. The Finance (SAP) system acknowledges the existence of the requested funding 4. The Workload Team Leader reviews the requisition and determines if it has the correct requisition coding. If it doesn't, the Workload Team Leader corrects the coding and the EPS solution re-assigns to the new Team Lead. When the requisition coding is correct, the Workload Team Leader reviews and assigns the requisition to a Contracting Office (CO) based on workload availability and required skill sets. 5. The CO reviews the requisition and collaborates with the Client (End User) as required. The CO will mentor the Client (End User) through EPS or through the preparation of the requisition including the industry engagement sub-process if required 6. With the collaboration of the CO, the Client (End User) determines the procurement type (as being either competitive or directed) for their procurement. This helps the Client (End User) determine which

	supporting information is required to be submitted with the requisition. 7. If the Client (End User) decides to proceed, they update the requisition and the supporting information for the selected procurement type, taking into consideration the Supplier responses to the industry engagement if applicable. 8. If the Client (End User) decides not to proceed the process proceeds to File Close Out. If the Client (End User) decides to make changes to their original request based on information as a result of the industry engagement, the process returns to the beginning of identifying the requirement. 9. The Client (End User) completes an initial procurement complexity and risk questionnaire which is used by EPS to determine an initial complexity and risk rating. The CO, using the EPS solution and the Client's (End User) completed complexity and risk questionnaire, determines the initial procurement complexity and risk ratings 10. The Client (End User) submits an updated requisition along with any/all supporting information 11. With the collaboration of the CO, the Client (End User) determines if there is a need to engage industry. When it is determined that Industry must be consulted, the CO prepares, in collaboration with the Client (End User), the engagement package using the EPS solution. Documents prepared by the CO for the engagement package are developed with and stored using the document management solution in EPS. The Supplier(s) respond to any engagement requests made by the Client (End User)/PWGSC/client dept via the engagement package using EPS. If industry engagement is required, once Supplier(s) engagement responses are received, the Client (End User) (in collaboration with the CO) reviews and analyzes the responses. 12. The process proceeds to the Procurement Planning & Strategy Development phase

Input	Description
Requisition	A requisition is sent to be managed.
Requisition from Shopping Cart Request	The requisition contained in the shopping cart for the request
Output	**Description**
Update Draft Requisition	Updated draft requisition with any supporting documentation
Updated Draft Requisition from Sourcing	The updated draft requisition from sourcing with any feedback/documentation

Draft Initial Procurement Complexity & Risk Rating	Risk rating is assigned to the requisition.

Business Rules

The Requisition Management business process is governed by the following rules:

1. The starting point of this process being "Client (End User) Sourcing Items" can come from the portal directly to sourcing or from the portal via a catalog search outcome (e.g. the Shopping Cart Request)
2. All required supporting information should accompany the requisition at the start of the process. As a minimum, the required attachments must include sole source limited tendering and certification, sole source justification (if applicable), price certification, supplier quotation, statement of work (SOW), initial privacy, procurement complexity and risk assessment.

b. Procurement Planning & Strategy Development

Process Model

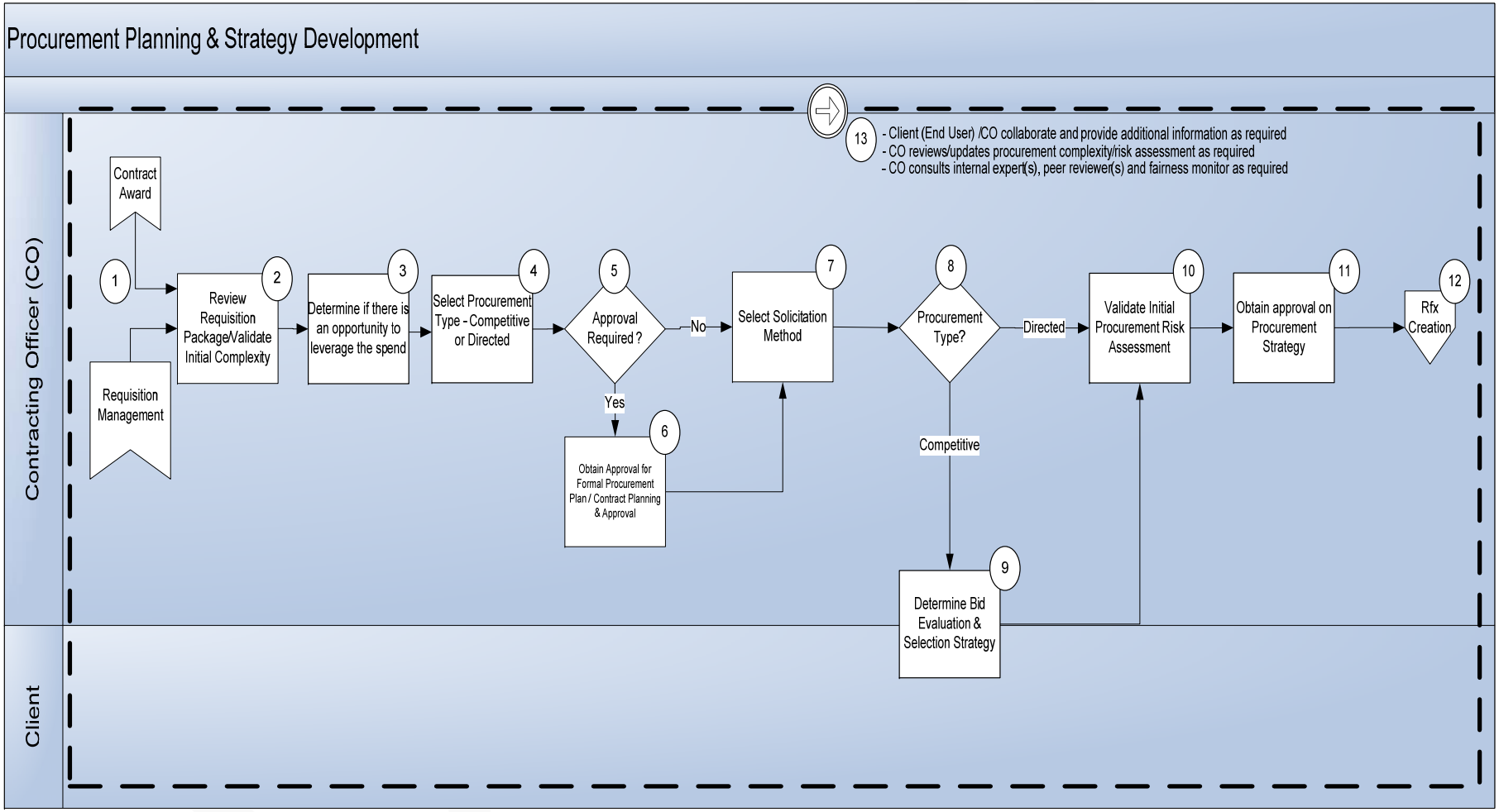


Figure 15 - Level 2 Procurement Planning & Strategy Development Business Process Model

Process Description

Procurement Planning and Strategy Development	
Summary Description	The purpose of the Procurement Planning & Strategy Development process is to plan, develop and prepare a strategy for procurement of goods/services. This sub-process includes steps to: • Review the requisition and supporting information such as the requirements, funding, security requirements, justification for sole source, competitive/directed procurement, and analyze options • Verify the statement of work • Identify environmental performance considerations such as contract policy, treaties and regulations, socio-economic conditions and trade agreements • Develop the procurement strategy including selecting the appropriate procurement vehicle • Review the evaluation criteria and selection methodology • Consult with internal/external experts as required (e.g. external experts such as market /commodity research information). • Approve the procurement strategy
Process Narrative ***Actors:*** • ***Contracting Officer***	The following process flow narrative pertains to Figure 15: 1. The Client (End User) has submitted their requisition and all supporting documents from the Requirements Definition phase or a request to re-tender a previous RFP has been made as a result of a change in scope from the previous RFP, change in funding or other reasons. The Manager/Supply Team Leader, using the EPS solution, acknowledges, to the Client (End User), receipt of the requisition and, using the Workload Management capabilities of the EPS solution, assigns the requisition package/procurement file using the approved requisition taxonomy coding (e.g. UNSPC). 2. The CO will then review the requisition and if needed, validate/update the procurement complexity as required. 3. The CO determines if there is an opportunity to leverage the "spend" by reviewing the procurement file and the procurement history of the commodities. The CO collaborates with the Manager and/or peers (such as commodity group experts) to determine if there is an opportunity to develop a procurement strategy to leverage the "spend". The CO uses any available history of buys for the respective commodities provided by the EPS solution. 4. The CO determines or confirms if the procurement type is competitive or directed. The CO also reviews "flags" displayed by the EPS solution, when one of the following criteria applies to the procurement file: a. Controlled Goods

b. Free Trade Agreements
c. Comprehensive Land Claim Agreements (CLCAs)
d. Procurement Strategy for Aboriginal Businesses (PSAB)
e. Risk Management Review
f. Vendor Performance (VPCM)
g. Procurement Review Committee (PRC/ACRO)
h. Security
i. Technical Expert Review
j. Need for Fairness Monitor

The CO will process the procurement file as per the areas that are flagged by the EPS solution including the inclusion of the fairness monitor into the process as required.

5. Whether or not flags are detected, EPS informs the CO if approval is required.
6. If required, the CO obtains approval for the formal procurement plan or the Contract Planning and Approval (CPAA).
7. The CO selects the solicitation method (which includes RFSAs and RFSOs). Templates for all required procurement documents are available from the EPS document management repository. At this step normally two types of procurement strategies are considered, a CPAA strategy and a formal procurement plan. The CPAA process involves preparation of the CPAA document/completing the form, notifying a manager if the CPAA procurement is sensitive or strategic and obtaining approval from the appropriate approval authority for the CPAA designated procurement as the required procurement strategy. The process for the formal procurement strategy is very similar with the exception that it does not involve completion of a form but rather production of a formal plan/strategy document. As well, normally the draft solicitation is produced simultaneously. Corporate communications provides input to the plan. The draft approval package is completed by the CO for review and recommendation by one or more of corporate communications, the supply team lead, manager and director. The package is forwarded to one or both of the senior director and the DGO for approval as well as at the DG and ADM levels as required. As well, at this step, consideration for the need of a fairness monitor is also taken into account by the CO. If required, the CO completes form 587, the ADM/AB reviews the form requesting a fairness monitor, and if approved request approval of the request from the BOC. The BOC will then in turn, seek approval from the ADM/DOB. If the request is denied at any of these three levels of approval, the CO records the details of the decision using the EPS solution. Once approved, the CO takes care of coordinating inclusion of the fairness monitor into the process.
8. Based on the identified procurement type being Competitive

	9. The CO reviews and finalizes, in collaboration with the Client (End User), the bid evaluation criteria, the selection method strategy and the Statement of Work (SOW) as required. 10. Regardless of the procurement type being competitive or directed, the CO, using the EPS solution, validates /updates the procurement risk assessment. 11. Regardless of the procurement type being competitive or directed, the CO, using the EPS solution, determines if the procurement strategy requires approval. The CO obtains approval for the procurement strategy by using the workflow processing capabilities of EPS to process the procurement file through the approval process based on the procurement file procurement risk rating 12. Once approvals are obtained, the CO proceeds to the Rfx Creation phase 13. Throughout the procurement strategy process, the CO & Client (End User) collaborate and provide additional information as required. The Procurement Complexity & Risk Assessment (PCRA) can be reviewed and/or updated throughout the process. As well, the CO determines if there is a need to consult with internal experts (such as costs analysts, legal services, risk management advisory services (RMAS), quality control (QC), communications, technical experts) on the procurement file. When there is a need to consult with internal experts the CO completes the workload assignment (using the Workload Management capabilities of EPS). The CO, using the EPS solution, then assigns/transfers the file to the required expert teams. The Internal Expert Managers/Team Leaders review the procurement file and using EPS assigns the file to experts that have the availability and skill-sets required. The experts will provide their input using the EPS solution. The CO, using the EPS solution, will re-assign the procurement file back to the CO who was last assigned. If required, the CO's Manager/Team Leader could also re-assign the procurement file to another CO within their organization.

Input	Description
Updated Draft Requisition (9200)	Updated draft requisition with any supporting documentation
Updated Draft Requisition from Sourcing	The updated draft requisition from sourcing with any feedback/documentation
Draft Initial Procurement Complexity & Risk Rating	Risk rating is assigned to the requisition.
Output	**Description**
Approved Procurement Plan,	The procurement plan is approved, evaluated and a strategy is selected before the Rfx Creation process

Evaluation & Selection Strategy	

Business Rules

The Procurement Planning & Strategy Development business process is governed by the following rules:

1. Determination of an optimal procurement strategy includes consultation with internal experts, peers and fairness monitor as required as well as referring to the Treasury Board Contracting Policy document (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14494&section=text) or the PWGSC supply manual (https://buyandsell.gc.ca/policy-and-guidelines/supply-manual) for relevant topics such as method of selection, basis of payment and bid evaluation procedures.
2. In this process, the principle questions asked are who, what, where, when, why and how pertaining to the procurement and resulting strategy, Therefore, consultation can occur with any subject matter expert (e.g. technical authority, contracting authority, legal services, communications) as required to develop all necessary questions.

c. Rfx (Solicitation) Creation

Process Model

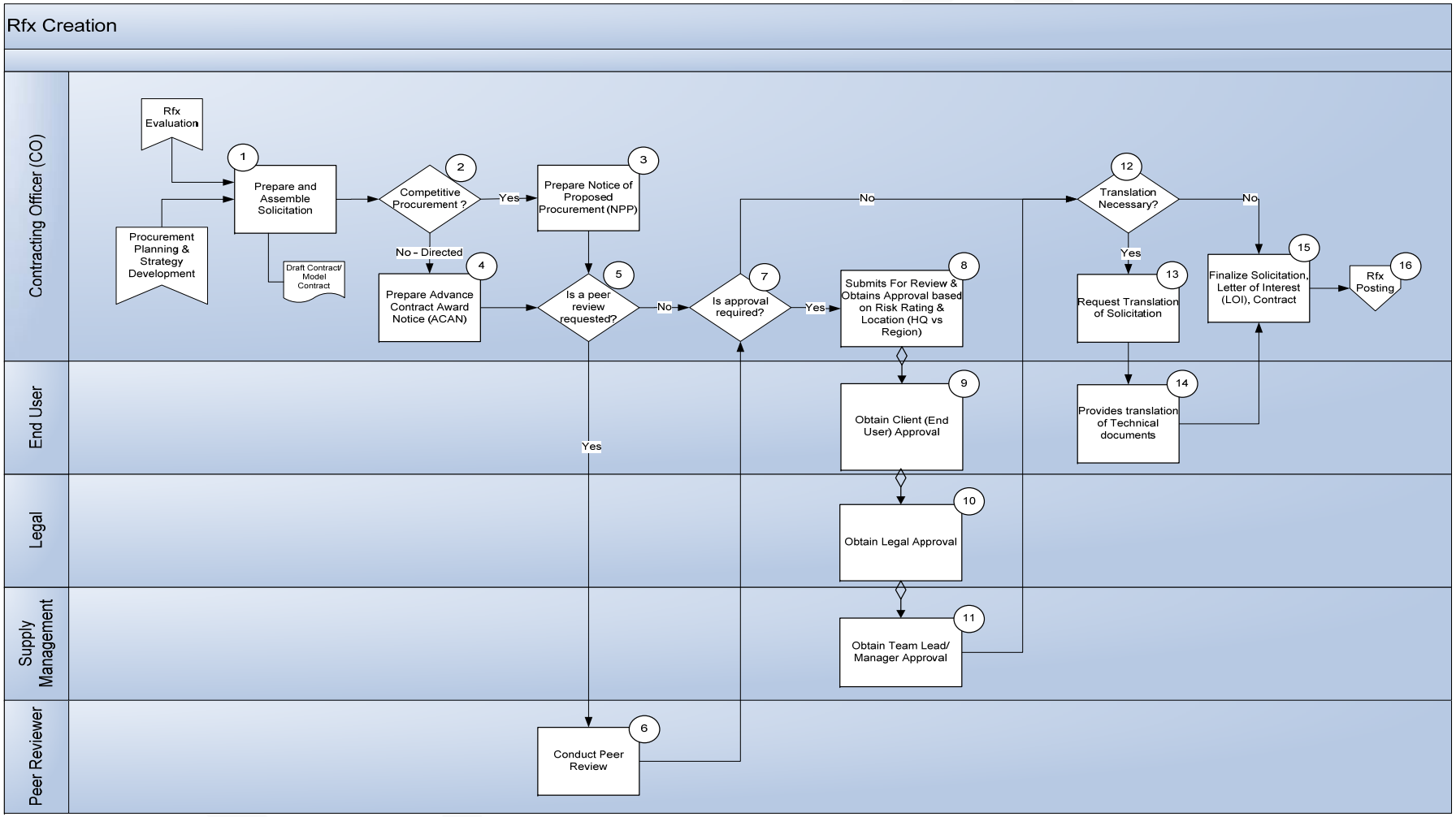


Figure 16 - Level 2 Rfx (Solicitation) Creation Business Process Model

Process Description

Rfx (Solicitation) Creation	
Summary Description	The purpose of the Rfx (Solicitation) Creation process is to (1) develop, and finalize the solicitation and (2) support the Supplier throughout the process. This sub-process includes steps to: • Develop the solicitation and bid notification • Manage the solicitation • Prepare solicitation amendments • Support Suppliers during the solicitation process
Process Narrative ***Actors:*** • ***End-user. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Legal*** • ***Supply Management*** • ***Peer Reviewer***	The following process flow narrative pertains to Figure 16: 1. The CO prepares and assembles the solicitation document as well as the draft\model contract (if and when required). 2. Based on the procurement type Competitive: 3. The CO prepares the Notice of Proposed Procurement (NPP) (if required) 4. If the procurement type is directed, the CO may prepare the advance contract award notice (ACAN) (Note: the outcome of an ACAN may result in a competitive process.) 5. The CO determines if a peer review is required/will be performed (Note: As part of the Procurement Strategy approval, the approval authority(s) can, as well, request a peer review) 6. Once it is determined if a peer review is required (and completed), the CO submits the procurement file for review. The CO, using the EPS solution, routes the procurement file for review through the review process. 7. Once the peer review is completed, the CO determines if approval is required 8. The CO or the Approval Authority (if required) submits and obtains approval based on the procurement file procurement risk rating and location. 9. Approval (if required) is obtained from the Client (End User) 10. Approval (if required) is obtained from Legal 11. Approval (if required) is obtained from the Team Lead/Manager 12. The CO determines if the approved solicitation requires translation. 13. When the approved solicitation requires translation, using the EPS solution, the CO requests from the Client (End User) the translation of the solicitation technical information. The CO also submits a translation request to the Translation Bureau for translation of the solicitation contractual components. 14. The Client (End User) provides translated technical documents to the CO.

	15. Once all the translated documents are received from the Client (End User) and the Translation Bureau, the CO finalizes the Solicitation, Letter of Interest (LOI) or draft of the contract. 16. The procurement file proceeds to the Rfx (Solicitation) process.

Input	Description
Approved Procurement Plan, Strategy, Evaluation & Selection Strategy	The procurement plan is approved, evaluated and a strategy is selected.
Output	**Description**
Finalized Translated Solicitation	Solicitation is finalized and translated in both official languages of Canada.

Business Rules

The Rfx (Solicitation) Creation business process is governed by the following rules:

1. Since the principle questions developed in the strategy that are answered in this process are who, what, where, when, why and how pertaining to the procurement, consultation can occur with any subject matter expert (e.g. technical authority, contracting authority, legal services, communications) as required.
2. Approval from the End User, Team Lead or Legal is conditional on the particulars of the procurement.
3. Rfx Creation and eventual Posting processes are governed by trade agreements and procurement vehicle tools. The following table is an example of tiered posting periods for two stage procurement of Professional Services:

	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	Directed Contracts (sole source up to 25k)	**Under NAFTA**	**From NAFTA to $2M**	**Over $2M**
Minimum # of Calendar Days for Posting	N/A	Clients are to determine the number of calendar days in accordance with the GCRs. It is recommended that you provide them a minimum of 5 calendar days.	15	20

Minimum of Suppliers Invited	N/A	Clients are to determine the number of suppliers invited in accordance with the GCRs. It is recommended that you invite a minimum of 2 suppliers.	15	All eligible suppliers
NPP Required	No	No	Yes	Yes

d. Rfx (Solicitation) Posting

Process Model

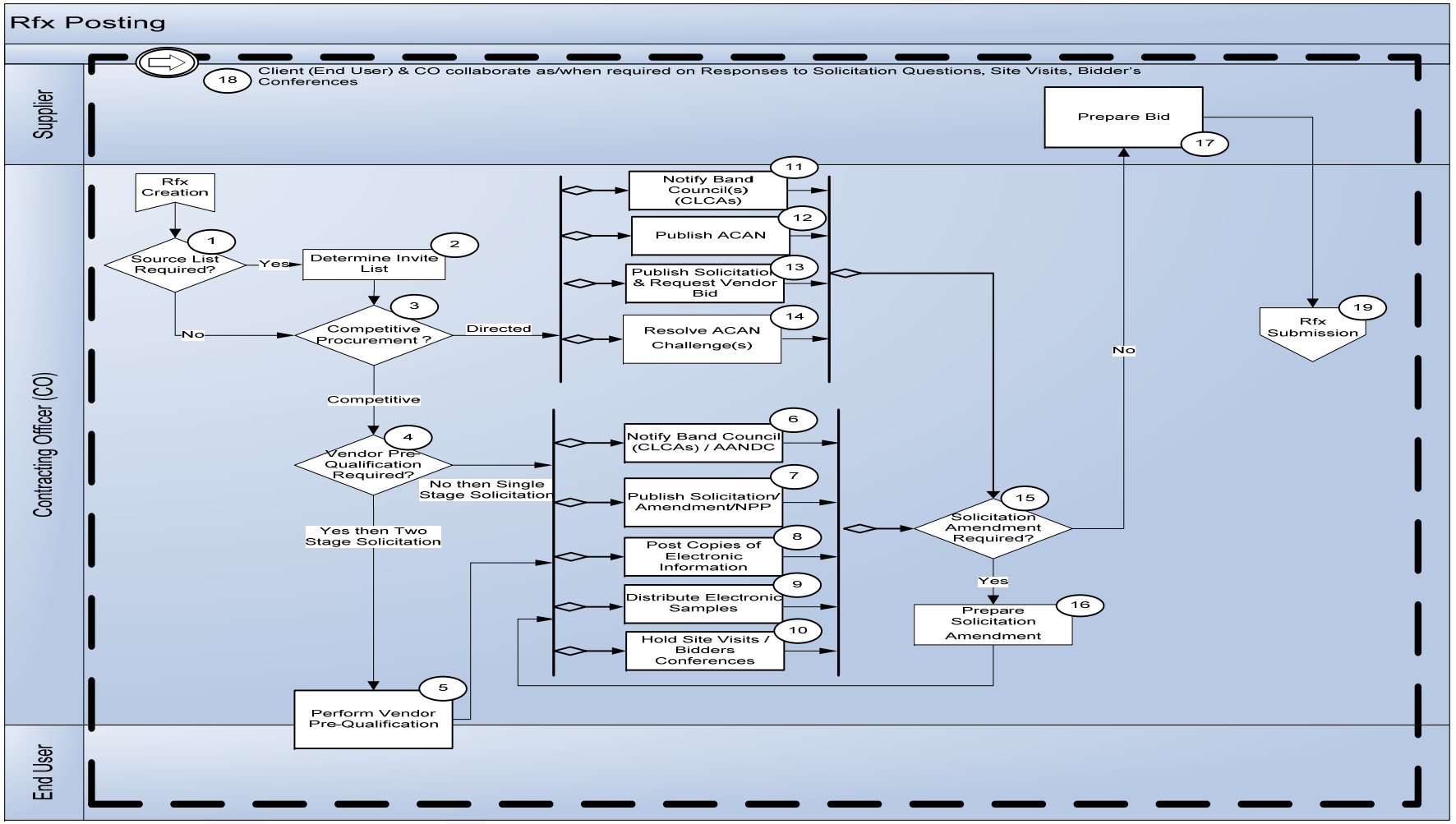


Figure 17 - Level 2 Rfx (Solicitation) Posting Business Process Model

Process Description

Rfx (Solicitation) Posting	
Summary Description	The purpose of the Rfx (Solicitation) Posting process is to (1) finalize and publish the solicitation (2) publish the bid notification including all amendments and (3) supporting the Supplier throughout the process. This sub-process includes steps to: • Publish the solicitation and bid notification to GETS • Manage the solicitation • Prepare and publish solicitation amendments • Support Suppliers during the solicitation process
Process Narrative ***Actors:*** • ***End-user. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Supplier***	The following process flow narrative pertains to Figure 17: Based on, 1. The CO determining whether or not a source list is required 2. If yes, the CO determines the content of an "Invite List" 3. Whether or not a source list is required, based on the procurement being, **Competitive**: 4. The CO determines, with the help of the procurement strategy, if the solicitation will be conducted in two stages: If the solicitation requires two stages: 5. The Client (End User) in collaboration with the CO performs the pre-qualification of Supplier(s). If the solicitation only needs to be conducted in one stage and after completing Vendor Pre-Qualification for a two stage solicitation: 6. For a procurement file for whom CLCAs may be applicable, the CO, using the EPS solution, notifies Band Councils listed on the CLCAs as per notification procedures contained within each Land Claim agreement. For a procurement file for whom PSAB applies, the CO, using the EPS solution, notifies Aboriginal Affairs and Northern Development Canada (AANDC). 7. As required, the CO, using the EPS solution, publishes the solicitation and/or solicitation amendments as well as the NPP to GETS Once the solicitation is posted: 8. The CO, using the EPS solution, posts copies of additional electronic information and 9. The CO, using the EPS solution, distributes electronic samples, as required. Physical samples are managed/tracked using EPS which includes the ability to record receipt of samples as part of bid receiving process 10. In collaboration with the Client (End User), the CO conducts site visits and bidders conference as required. **Directed**:

	11. For procurement files for whom CLCAs apply, the CO, using the EPS solution, notifies Band Councils listed on the CLCAs as per notification procedures contained within each Land Claim agreement. 12. The CO, using the EPS solution, publishes the ACAN to GETS. Note: this step is discretionary since we do not have to publish ACANs if we are using a National Security Exemption (NSE) or when CO is confidant of sole sourcing (IP rights). 13. The CO, using the EPS solution, solicits the Supplier for a bid by publishing the solicitation to GETS for Supplier review or sending email notifications asking for Supplier submissions. The Supplier submits their bid(s) based on their interest in the solicitation. 14. The CO, using the EPS solution, processes all received ACAN challenges. This involves the CO reviewing the details of all challenges that were submitted by the challenger within the specified timeframes and consulting with the Client (End User) to collaboratively prepare recommendation(s) for either acceptance or rejection of any challenge. Any challenges that are accepted, using the EPS solution, the CO notifies (a) the Client (End User) that competition for the procurement will occur, as well as (b) the challenger and (c) the sole source supplier that the procurement requirement will be competed. Using the EPS solution, the CO records details of the decision. Any rejected challenges are reviewed by the appropriate authorities which may include the Manager at level 1, the Director at level 2, the Director General and/or Regional Director General at level 3 and then the ADM at level 4. If agreement for rejection is obtained at any of these levels, using the EPS solution, the CO notifies the Client (End User) and challenger as well as records details of the decision. If disagreement for rejection is obtained at any of these levels, effectively accepting any challenge, using the EPS solution, the CO notifies (a) the Client (End User) that competition for the procurement will occur, as well as (b) the challenger and (c) the sole source supplier that the procurement requirement will be competed. Using the EPS solution, the CO records details of all decisions regarding ACAN challenges. 15. As required, the CO determines the need for a solicitation amendment 16. As required, the CO prepares solicitation amendment for publishing. Addressing an amendment involves the EPS solution creating a notice of amendment on behalf of the CO and the CO addressing any changes to the procurement strategy resulting from the solicitation amendment. If changes to the strategy are required, the procurement risk assessment is updated by the EPS solution and reviewed by the CO. The procurement strategy is also reviewed by the CO for consideration of obtaining approval as required. If the solicitation amendment results in a change to the bidding period, using the EPS solution, the CO notifies the BRU of the change to the bid closing date. On behalf of the CO, the EPS solution will also request a translation of the solicitation amendment to finalize the amendment

	17. Once the solicitation is published the Supplier prepares their bid and submits questions related to the solicitation. 18. The CO collaborates with the Client (End User) on responses to solicitation questions as well as site visits and bidder's conferences. 19. The procurement file proceeds to 5.0 Rfx (Solicitation) Submission

Input	Description
Finalized Translated Solicitation	Solicitation is finalized and translated in both official languages of Canada.
Output	**Description**
Published/Posted Solicitation	A published and posted solicitation.
Supplier Provided Bid	Supplier provides a bid for the solicitation
Finalized Translated Solicitation Amendment	Any changes to the solicitation are made and are translated in both official languages of Canada.

Business Rules

The Rfx (Solicitation) Posting business process is governed by the following rules:

1. The Rfx Posting process is governed by the solicitation closing date which also governs the time period for Supplier issuing questions and PWGSC responding to questions.
2. The Rfx Posting process is governed by trade agreements and procurement vehicle tools
3. The publishing steps in this process involve publishing to the existing Buy and Sell GETS site. Therefore, the publishing steps in this process are governed by the publishing rules of the GETS site publishing process.

e. Rfx (Solicitation) Submission

Process Model

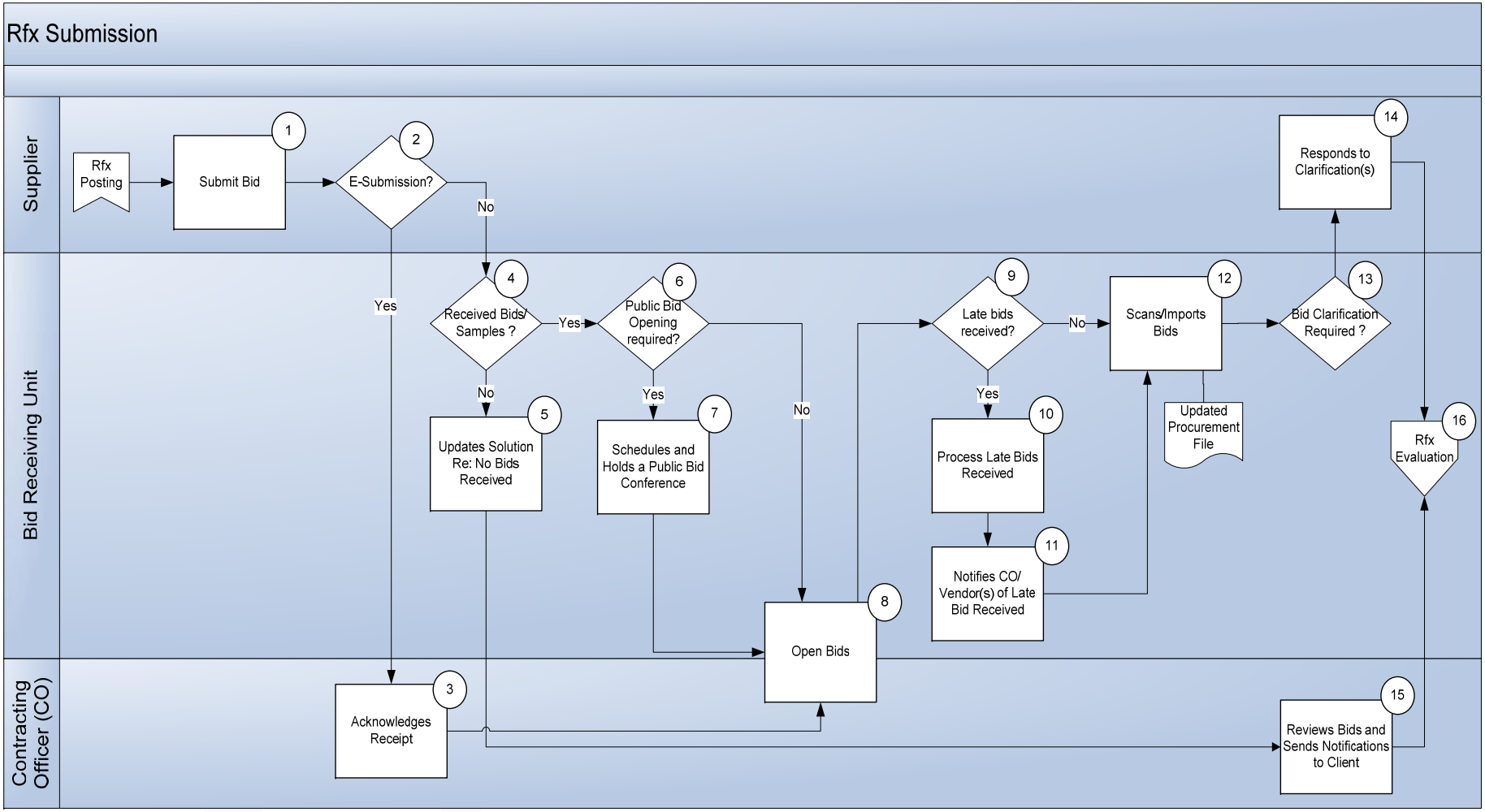


Figure 18 - Level 2 Rfx (Solicitation) Submission Business Process Model

Process Description

Rfx (Solicitation) Submission	
Summary Description	The purpose of the Rfx (Solicitation) Submission process is to submit and process the receipt of bids. This sub-process includes steps to: • submit & receive bids manually and electronically • conduct public opening of bids and/or bidders conferences when required • dealing with late bids • requesting and processing bid clarifications
Process Narrative ***Actors:*** • ***Bid Receiving Unit (BRU)*** • ***Contracting Officer*** • ***Supplier***	The following process flow narrative pertains to Figure 18: 1. The Supplier submits paper or electronic bids by the solicitation's bid closing date/time for competitive and directed solicitations 2. For electronic submissions, the Bid Receiving Unit (BRU), using the EPS solution, 3. Acknowledges receipt of the bid. Suppliers who submit bids electronically receive an acknowledgement notice from the BRU, using the EPS solution. For hand delivered submissions, the BRU provides a receipt for each bid. 4. Using the EPS solution, the BRU receives either or both of paper and electronic bids as well as samples which are matched with their respective bids. 5. If applicable, once the bid solicitation period is closed, the BRU updates the EPS solution if no bids have been received 6. Once the bid solicitation period is closed, the BRU determines if a public bid opening is required for any or all bids received. 7. If required, a public bid opening conference is scheduled & conducted 8. The BRU along with the CO opens/views all paper and/or electronic bids 9. When bids are received late, 10. The BRU updates the EPS solution to indicate that late bids were received. Using the EPS solution, the BRU prepares a late bid letter and returns all late bids to the Supplier(s). 11. Using the EPS solution, the BRU notifies the CO that late bids were received. 12. For all acceptable paper bids, the BRU scans and inserts the scanned bid into the EPS solution. For all acceptable electronic bids, the BRU using the EPS solution uploads them electronically into EPS. In either case, the procurement file is updated. 13. The BRU determines if any bid clarifications are required and requests clarifications from the Supplier(s). 14. The Suppliers respond to all requests for clarifications 15. The CO reviews all bids and send all notifications re: bids received/not received/late/non-compliant to the Client

	16. The procurement file proceeds to the Rfx (Solicitation) Evaluation process.

Input	Description
Published/Posted Solicitation	A published and posted solicitation.
Supplier Provided Bid	Supplier provides a bid for the solicitation
Finalized Translated Solicitation Amendment	Any changes to the solicitation are made and are translated in both official languages of Canada.
Output	**Description**
Supplier Bid	Supplier completes a bid for the solicitation.
Supplier Bid Clarification	Any issues or comments regarding the Suppliers bid are clarified.
Late Bid Notifications	Notifications are sent to the Supplier based on late bids.

Business Rules

The Rfx (Solicitation) Submission business process is governed by the following rules:

1. The solicitation start and bid closing dates

f. Rfx (Solicitation) Evaluation

Process Model

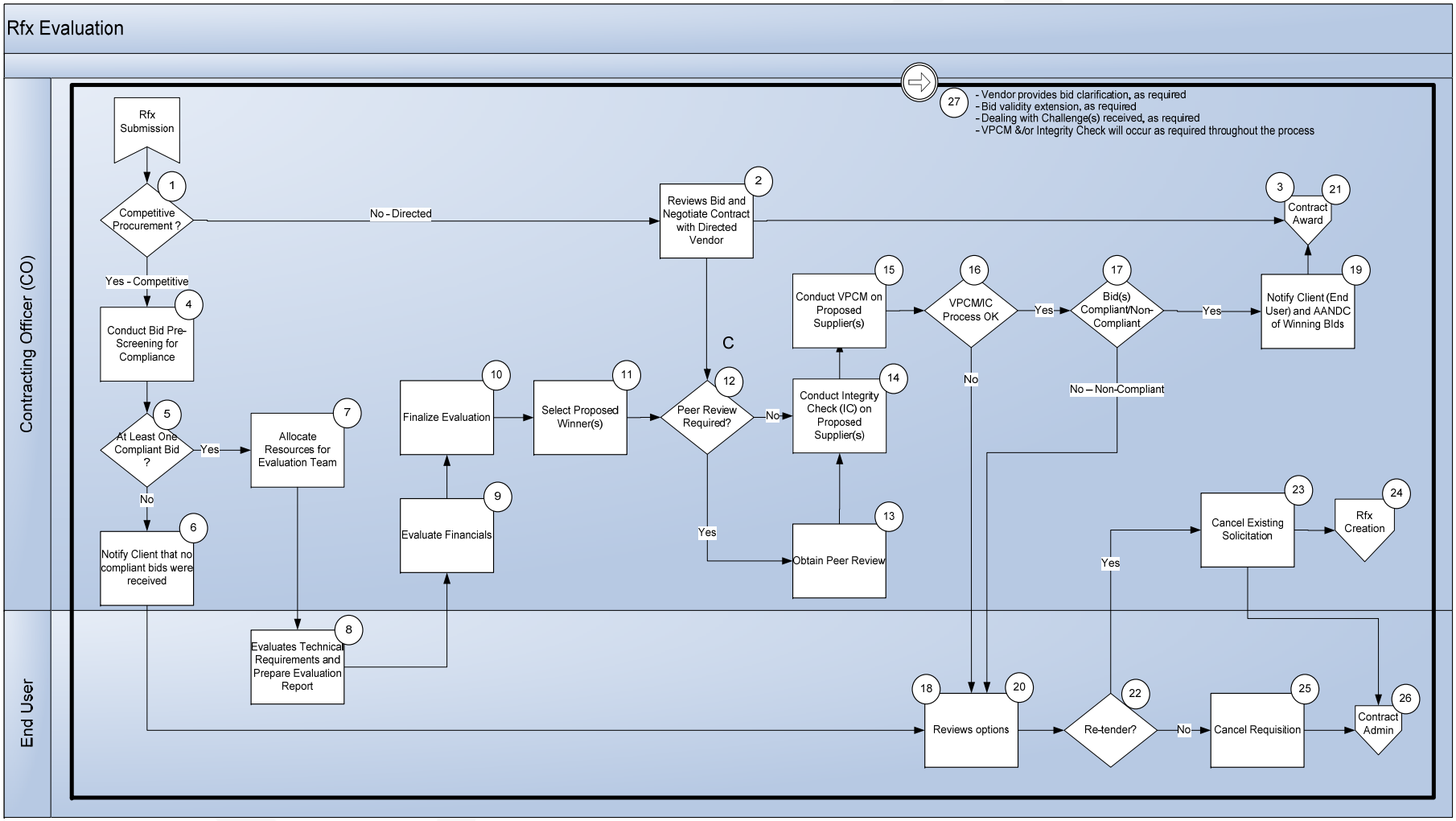


Figure 19 - Level 2 Rfx (Solicitation) Evaluation Business Process Model

Process Description

Rfx (Solicitation) Evaluation	
Summary Description	The purpose of the Rfx (Solicitation) Evaluation process is to evaluate bids and select the proposed winner(s). This sub-process includes steps to: • electronically pre-screen and tabulate bids • evaluate bids with EPS tool support • select a proposed winner(s)
Process Narrative ***Actors:*** • ***End-user. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer***	The following process flow narrative pertains to Figure 19: 1. For bids received for directed solicitation(s), 2. The CO reviews the solicitation and negotiates the contract with the Supplier. The Client (End User) could provide assistance to the CO in determining if costs are reasonable or reflective of efforts provided in delivering work. The CO will notify the Client (End User) of successful conclusion to contract negotiations as required. 3. After completion of contract negotiations, the process proceeds to Contract Award For bids received for competitive solicitation, 4. For both electronic and manually submitted bids, the CO, using the EPS solution, conducts bid pre-screening for compliance. This involves (a) tabulation of mandatory, financial and technical responses, as required, (b) sending notifications when the tabulation is completed (c) CO reviewing the mandatory requirements tabulation (d) CO validating the tabulation results in the EPS solution as required (e) checking for compliance regarding technical & financial certification as well as security, insurance and employment equity certification, CLCA and AANDC certification (f) under a Supply Arrangement (SA) scenario, ensuring that pre-qualified suppliers are able to bid 5. If no bids received are compliant, 6. The CO, using the EPS solution, informs the Supplier(s) and the Client (End User) that no complaint bids were received and options are reviewed at (18) 7. When at least one compliant bid(s) is received, the CO allocates/assigns resources to the evaluation team 8. The CO submits the technical portion of the bids as well as all bid amendments and supplier questions to the Client (End User) using the EPS solution. The Client (End User) leads the technical evaluation but the CO may participate in this part of the evaluation. Once the technical evaluation is completed, the Client (End User) may prepare and submit a technical evaluation report to the CO using the EPS solution. The CO oversees, coordinates and reviews the technical evaluation, as required. 9. The CO evaluates the bid's financial portion only for those supplier bids that are deemed to be technically compliant. Legal may be

	consulted for legal issues. Cost analysts could be consulted to determine financial viability of the proposed contractor. 10. The CO finalizes the evaluation including technical & financial certification as well as security, insurance and employment equity certification. 11. The CO selects a proposed winner(s) 12. The CO determines if a peer review is required. 13. If required, the CO obtains peer review using the workflow capabilities of the EPS solution. The peer reviewer looks at the results of the bid evaluation and makes a comparison to the original solicitation. If issues are found, the peer reviewer discusses issues with the CO & signs the approval. All outstanding issues are resolved by the CO supervisor. 14. Whether or not a peer review is required, the CO requests an integrity check on the proposed winner(s). This process, also referred to as the "Integrity Provisions (Code of Conduct) process, can involve the CO, using the EPS solution, requesting from the Supplier consent for a criminal record check. The Supplier completes form 229, which is then reviewed for completeness by the CO using the EPS solution, and forwarded to DOB/SID who in turn interface with the RCMP for criminal record checking (e.g. checking for the existence of criminal convictions). If none are found, DOB/SID, using the EPS solution, notifies the CO and the step is completed with all decisions recorded. If convictions are found, DOB/SID, using the EPS solution, notifies the CO, who in turn notifies Senior Management in the appropriate department/sector. If the CO decides to disqualify the Bidder/Supplier and Senior Management agrees with the CO's decision, the CO identifies them as non-compliant. If Senior Management disagrees with the CO's decision to disqualify the Bidder/Supplier, Senior Management must approve the decision to continue with the Bidder/Supplier. The step is complete once all decisions are recorded in the EPS solution. 15. The CO, using the EPS solution, will check for any Vendor/Supplier performance issues (VPCM process). If any are found, the CO analyses the circumstances further by determining whether the terms of reference of the previous performance context are applicable to the current procurement scenario. If the CO determines that they do not apply, the step is complete with all conclusions recorded in the EPS solution. If the CO determines that the terms of reference of the previous performance context are applicable to the current procurement scenario, using the EPS solution, the CO can either reject the bid or forward a justification to contract with the Vendor/Supplier to the Director General/Regional Director General (DG/RDG) for their review. This justification will be based on any exceptional factors such as there being an insufficient amount of time to re-compete the solicitation. The DG/RDG will either recommend making an exception to the underlying performance issues or agree with rejection of the bid. If the bid is rejected, using the EPS solution, the CO notifies the

	Vendor/Supplier and the step is completed once all decisions are recorded in the EPS solution. If the DG/RDG recommends making an exception to the underlying performance issues, they forward their recommendation to the ADM level using the EPS solution. The ADM will either approve the exception or agree to reject the bid. In either case, the DG/RDG & the CO are informed, decisions/reasons are recorded in the EPS solution and the step is complete. Note that in a departmental sector or region, the above ADM level will be the appropriate designated approval authority. 16. The CO processes the procurement file based on the results of the VPCM process and the results from the criminal record check including determining the course of action based on the VPCM process and/or the criminal records check. Once evaluation is finalized, the VPCM and/or the criminal record check process is confirmed to be completed successfully 17. If the VPCM/CRC and/or the criminal record check process is successful, the bid is confirmed to be compliant or not compliant 18. When the VPCM process or the criminal record check has a negative outcome, the Client (End User) assesses/reviews their options, in collaboration with the CO 19. If the compliant or not compliant check confirms the existence of a compliant bid, the CO, using the EPS solution, notifies the Client (End User) and AANDC of a winning bid. 20. If the compliant or not compliant check has a negative outcome regarding the existence of a compliant bid the Client (End User) assesses/reviews their options, in collaboration with the CO. 21. After confirmation of a compliant bid, the procurement file proceeds to the Contract Award process 22. Once the Client (End User) assesses/reviews their options, in collaboration with the CO, they determine if they would like to re-tender the solicitation 23. When the Client (End User) decides to re-tender , they cancel the existing solicitation including notifying all bidders of the cancellation as required and 24. The procurement file returns to the Rfx Creation process 25. When the Client (End User) decides not to re-tender and decides to no longer procure the commodity, they cancel the original requisition including notifying all bidders of the cancellation as required and 26. The procurement file proceeds to the contract administration procurement file close-out process 27. Throughout the bid evaluation process, the CO assesses the requirement for extending the validity of a Supplier(s) bid as required and deals with bid challenges that have been received from Suppliers. As well Suppliers provide to the CO all bid clarifications as and when requested throughout the bid evaluation process. The process of managing bid clarifications involves the CO (a) receiving clarifications from the bidder(s) (b) disseminating the clarifications internally to the client (end user) and all other interested parties (as required) (c)

	ensuring clarifications received do not result in a “bid repair” which results in rejection of the clarification and requesting a new clarification

Input	Description
Supplier Bid	Supplier completes a bid for the solicitation.
Supplier Bid Clarification	Any issues or comments regarding the Suppliers bid are clarified.
Output	**Description**
Selected Winning Bid	The winning bid is selected from a list of Suppliers.
Negotiated Contract	The contract may be negotiated between the CO and Supplier.
Cancelled Solicitation	The solicitation is cancelled.
Cancelled Requisition	The requisition is cancelled.

Business Rules

The Rfx (Solicitation) Evaluation business process is governed by the following rules:

1. A fairness monitor can be present during the evaluation process. Please refer to the Treasury Board Contracting Policy document (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14494&section=text) for more information.

g. Contract Award

Process Model

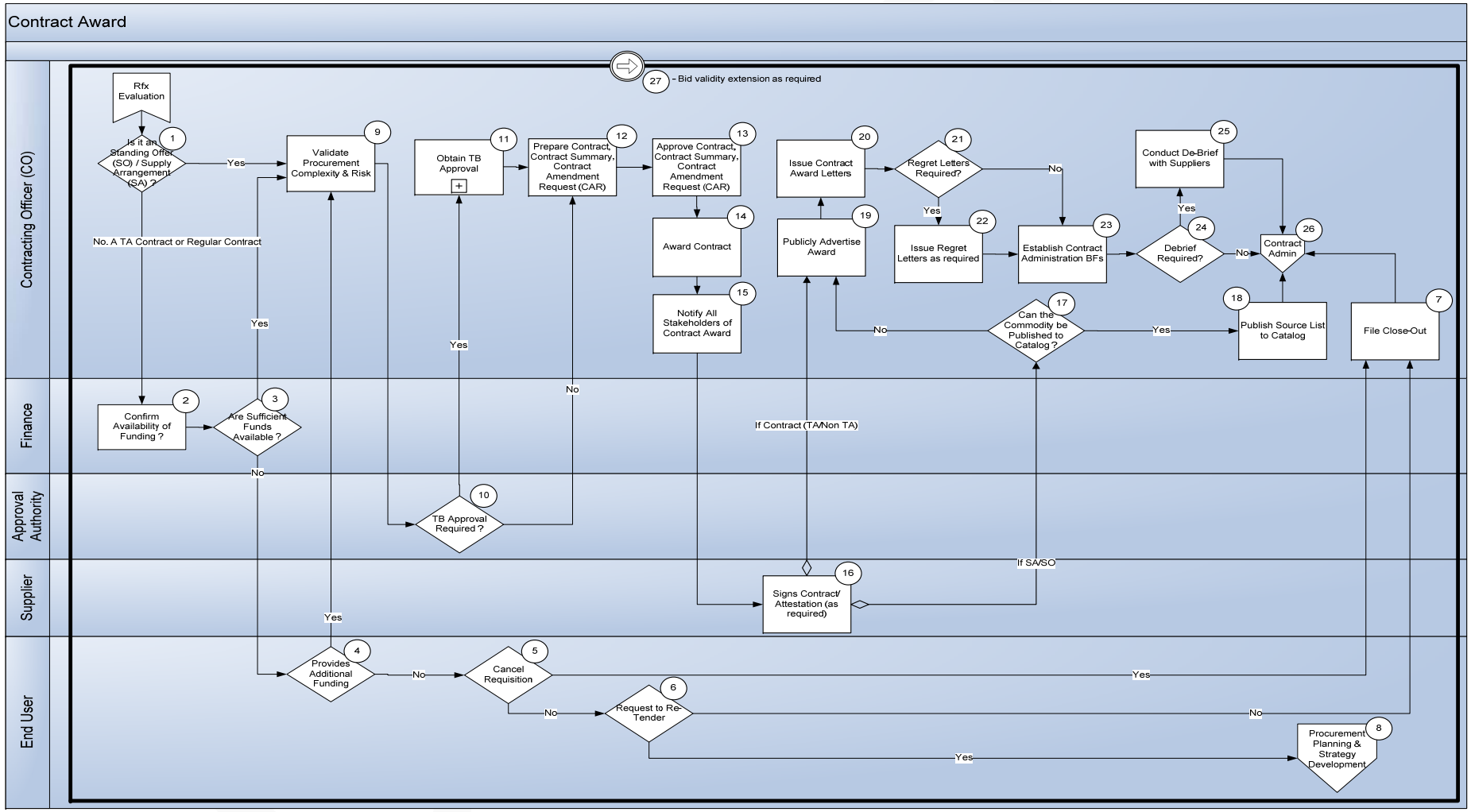


Figure 20 - Level 2 Contract Award Business Process Model

Process Description

Contract Award	
Summary Description	The purpose of this Contract Award sub-process is to award the contract to the selected proposed winner(s). This process includes steps to: • Confirm funding availability • Prepare the contract • Award the contract • Publically advertise contract awards
Process Narrative ***Actors:*** • ***End-user. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Supplier*** • ***Approval Authority***	The following process flow narrative pertains to Figure 20: 1. The EPS solution, on behalf of the CO, determines if the contractual context pertains to a Standing Offer (SO) or a Supply Arrangement (SA). If yes, the process proceeds to step 6 to validate procurement complexity and risk. If no, then the contractual context proceeds to step 2. 2. If the contractual context pertains to a Task Authorization (TA) or a Regular Contract, the CO confirms, with the assistance of Finance, if there are sufficient funds allocated for the total dollar amount from the original requisition. 3. If the requisition does have sufficient funds, the process proceeds to step 6 to validate the procurement complexity and risk. If the requisition does not have sufficient funds the process proceeds to step 4. 4. If the Client (End User) provides additional funds, they get allocated to the requisition/solicitation and the process proceeds to step 6 to validate the procurement complexity and risk. In some instances, Client (End User) departments may be issuing a Section 41 (Hard Commitment) at this step. 5. If the Client (End User) cannot provide additional funds, the Client (End User) can cancel the requisition. 6. If the Client (End User) does not cancel they can then decide to re-tenders the requisition/solicitation, 7. If the Client (End User) cancels the requisition/solicitation, or decides not to re-tender, the CO closes the procurement file 8. If the Client (End User) decides to re-tender, the process returns to the Procurement Planning & Strategy phase of the process. 9. If sufficient funds are available, or the Client (End User) provides additional funding, the CO, using the EPS solution, validates the Procurement Complexity and Risk. The EPS solution will update the procurement risk rating. 10. If applicable, the CO determines if Treasury Board approval is required. 11. The CO obtains Treasury Board approval as required.

	12. If Treasury Board approval is not required or once Treasury Board approval has been obtained, the CO prepares the contract, contract summary and/or the contract amendment request as required using the EPS solution. The CO also prepares/assembles the contract approval package and consults with corporate communications if the procurement is sensitive and/or strategic. The CO also validates the Supplier's security requirements and re-confirms that there are no VPCM's that exist against the Supplier. 13. The CO uses the workflow capabilities of the EPS solution to obtain the contract or the contract amendment request approval and signature (as required) based on the authority required for the procurement risk rating of the procurement file. 14. Once the contract is approved and signed internally, the CO awards the contract including issuing/establishing the Standing Offer (SO) or the Supply Arrangement (SA) if applicable. 15. The CO notifies all stakeholders of contract award 16. The CO then obtains the signature(s) for the contract/attestation from the selected winner(s) (as required). The CO updates the EPS solution to indicate that the contract is awarded. In some cases, EPS will award the contract using e-signatures. 17. The CO, using the EPS solution, determines if the procurement method is an RFSA or RFSO. If an existing RFSA/RFSO applies, the CO, using the EPS solution, determines if the commodity can be published to a catalogue. 18. If the commodity can published to a catalogue, the CO, along with the winning Supplier, will publish the source list and the catalogue items to the EPS solution catalog. 19. If the commodity cannot be published to a catalogue or if an existing RFSA/RFSO does not apply, the CO, using the EPS solution, publically advertises the contract award 20. The CO prepares contract award letters, using the EPS solution, and issues copies to the Supplier(s). 21. The CO determines if regret letters are required 22. If they are, the CO prepares the regret letters, using the EPS solution, and issues copies to the Supplier(s). 23. The CO establishes the contract administration BFs in the EPS solution 24. The CO determines if a de-brief is required, 25. If a de-brief is required, the CO conducts a debrief with the suppliers. 26. Whether or not a de-brief is required, the process proceeds to Contract Administration 27. At any point in the process, the CO determines and processes any bid validity extensions as required.

Input	Description
Selected Winning Bid	The winning bid is selected from a list of Suppliers.

Negotiated Contract	The contract may be negotiated between the CO and Supplier.
Cancelled Solicitation	The solicitation is cancelled.
Cancelled Requisition	The requisition is cancelled.
Output	**Description**
Procurement File Closed	The procurement file is closed.
Awarded/Signed Contract	The contract has been awarded and signed by the Supplier.
Created/Updated Catalogue Entry	The catalogue entry is updated or created based on prior information
Regret Letter(s)	Regret letters sent to unsuccessful Suppliers.
Contract Administration Bring Forwards (BFs)	
Publicly Advertised/Posted Contract Award	Contract Award is publicly advertised and posted.
Supplier De-Briefing(s)	Supplier is de-briefed.

Business Rules

The Contract Award business process is governed by the following rules:

1. In cases of contract award for procurement of resources, security levels of the proposed resources in the winning bid are verified early in this process and prior to contract awarding.
2. For more information regarding contract award rules, please refer to the Treasury Board Contracting Policy document (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14494&section=text) for more information.

h. Contract Administration

Process Model

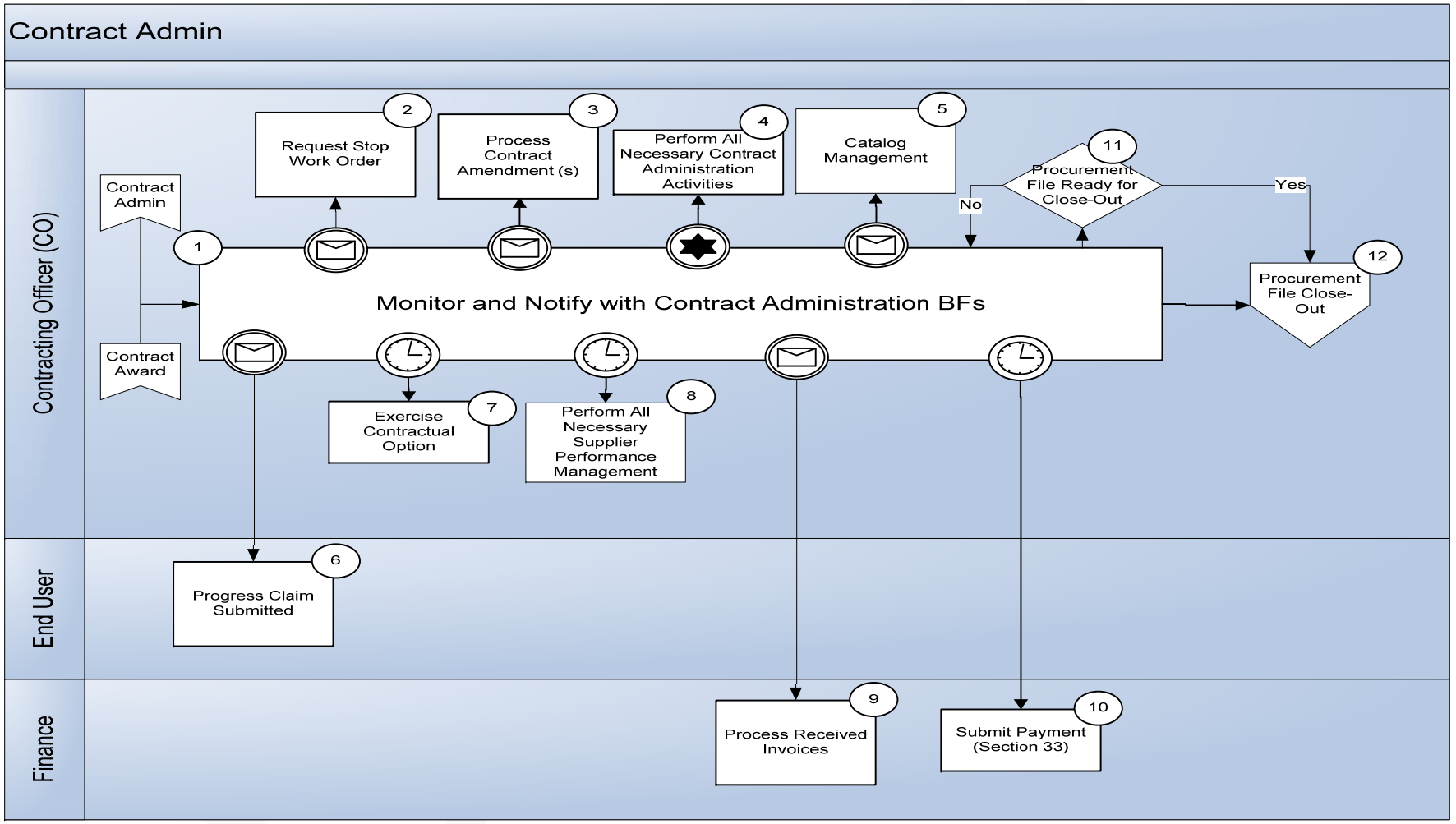


Figure 21 - Level 2 Contract Administration Business Process Model

Process Description

Contract Administration	
Summary Description	The purpose of this Contract Administration sub-process is to monitor and evaluate the execution of contract lifecyle management. This sub-process includes steps to: • Action Design Change Request • Action RPS Change Work Order Request • Amend the Contract • Apply Vendor Performance Corrective Measure • Assignment of Contract • Conduct Benchmark Testing • Conduct Delivery Follow-up • Contract Suspension • Ensure Sealed Sample(s) Returned • Ensure Security Deposit Returned • Evaluate Pre-Production Samples • Evaluate Supplier Performance • Financial Audit Required • Hold Post-Award Meeting • Hold Progress Review Meeting • Issue Task Authorization(s) • Manage Additional Work Requirements • Manage/Resolve Conflicts/Issues • Monitor Spending • Monitor Warranty • Profit Negotiations • Rate Review Meeting and Rate Negotiations • Reconcile Government Supplied Material • Remind Client of Need for a New Requisition for a Follow-On Contract • Respond to Audit Request • Terminate Contract • Time Verification
Process Narrative ***Actors:*** • ***End-user. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer***	The following process flow narrative pertains to Figure 21: Using the EPS solution, the CO: 1. Monitors contract administration BFs and provides notifications, in advance, when contracting administration BFs are coming due 2. Using the EPS solution, the Client (End User) requests stop work orders as required 3. The CO determines if contract amendments are required. If yes, the CO prepares and obtains sign-off on contract amendments and conducts all necessary contract administration activities as required pertaining to amendments

4. Using the EPS solution, the CO performs any of the following contract administration activities as required:

- Action Design Change Request
- Action RPS Change Work Order Request
- Amend the contract
- Apply Vendor Performance Corrective Measure
- Assignment of Contract
- Conduct Benchmark Testing
- Conduct Delivery Follow-up
- Contract Suspension
- Ensure Sealed Sample(s) returned
- Ensure Security Deposit returned
- Evaluate Pre-Production Samples
- Evaluate Supplier Performance
- Financial Audit Required
- Hold Post-Award Meeting
- Hold Progress Review Meeting
- Issue Task Authorization(s)
- Manage additional work requirements
- Manage/Resolve Conflicts/Issues
- Monitor Spending
- Monitor Warranty
- Profit Negotiations
- Rate Review Meeting and Rate Negotiations
- Reconcile Government Supplied Material
- Remind Client of need for a new Requisition for a follow-on contract
- Respond to Audit Request
- Terminate Contract
- Time verification

5. Using the EPS solution, the CO performs any catalogue management tasks as required
6. Using the EPS solution, the Supplier submits progress claims to the Client (End User).
7. Using the EPS solution, the Client (End User) exercises contractual options.
8. The CO performs all necessary supplier performance management tasks
9. Finance processes all received invoices
10. Finance submits payments (Section 33)
11. The CO determines if the procurement file is ready for close-out. If the file is not ready for close-out, the process returns to step 1 Monitor Contract Administration BFs for continued contract administration monitoring
12. Once the file is ready for close-out, the process proceeds to step 12 Procurement File Close-Out.

Input	Description
Contract Administration Bring Forwards (BFs)	Notifications of Contract Administration Tasks/Events
Output	**Description**
Request Notification to Close Procurement File(s)	The CO requests and notifies of the closure of the Procurement File(s).

Business Rules

The Contract Administration business process is governed by the following rules:

1. Any Contract Administration process is governed by events based on time, financial, contractual delivery and ad-hoc events as well as Statement of Work (SOW) tasks.

i. Procurement File Close-Out

Process Model

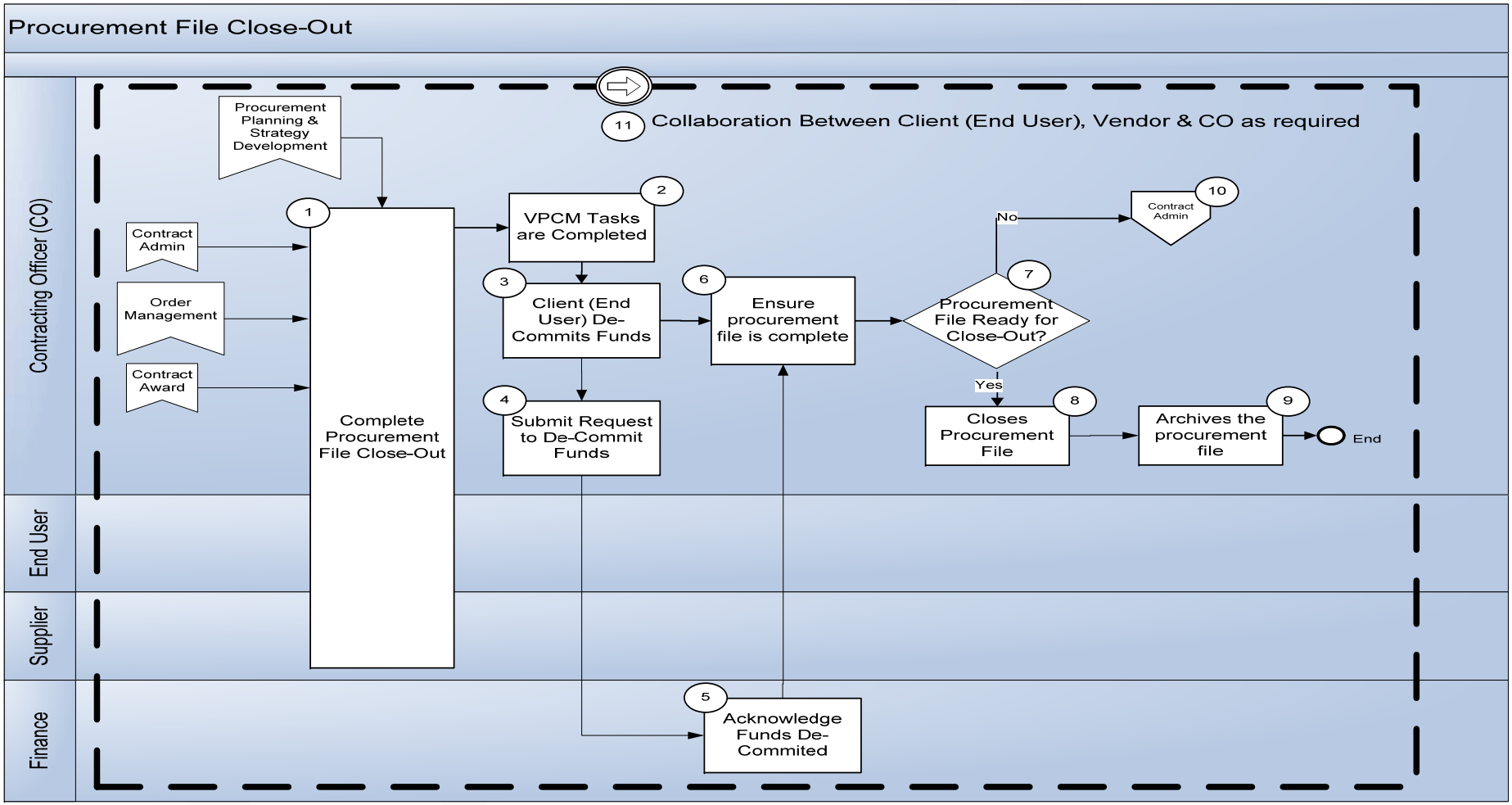


Figure 22 - Level 2 Procurement File Close-Out Business Process Model

Process Description

Procurement File Close-Out	
Summary Description	The purpose of this Procurement File Close Out process is to complete and close the procurement file. This sub-process includes steps to ensure that, • contract deliverables were delivered • all issues are resolved • applicable warranty is over • all invoices are paid • final Supplier performance evaluation is conducted and • the procurement file is archived according to records management policy
Process Narrative ***Actors:*** • ***End-User. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Supplier***	The following process flow narrative pertains to Figure 22 : Using the EPS solution, the CO: 1. completes the procurement file close-out by, i. Determining when the final Supplier performance evaluation is conducted ii. Determining when the warranty period is over iii. Listing all invoices/progress claims that are paid iv. Determining when all contractual deliveries are completed v. Ensuring that there are no Unresolved Issues (e.g. returning bid security cheques/bonds if applicable vi. Ensuring that all required forms were completed (e.g. CPERF in construction) vii. Ensuring that GFM and Tooling is returned viii. Ensuring that the Contract is Complete 2. The CO also ensures that all tasks re: Vendors Performance Corrective Measures (VPCM) are completed. 3. The CO also ensures that de-committing of funds is completed by the Client (End User) if there are financial commitments that remain. 4. The CO submits a request to Finance to de-commit the funds if there are financial commitments that remain. 5. Finance de-commits fund if there are financial commitments that remain and sends an acknowledgement to the CO via the EPS solution. 6. The CO ensures that the procurement file contains all required information 7. The CO confirms that the procurement file can be closed and archived When the procurement file is ready to be closed: 8. Using the EPS solution, the CO closes the procurement file 9. Using the EPS solution, the CO archives the procurement file When the procurement file is **not** ready to be closed: 10. The CO continues to perform contract administration10

	11. Collaboration occurs between the CO, Supplier and Client (End User) as required throughout the process.

Input	Description
Request/Notification to Close Procurement File(s)	The CO requests and notifies of the closure of the Procurement File(s).
Output	**Description**
Closed/Archived Procurement File(s)	Procurement File(s) closed archived for future reference.

Business Rules

The Procurement File Close Out business process is governed by the following rules:

1. Departmental archival policies, practices and standards.
2. De-committing of funds must occur on all the respective cost centres applicable to the original procurement request when closing the procurement file
3. All correspondence, especially email must be included in the procurement file.

8.2. Level 3 Business Process Models and Descriptions

a. TB Submission Approval (Part 1)

Process Model

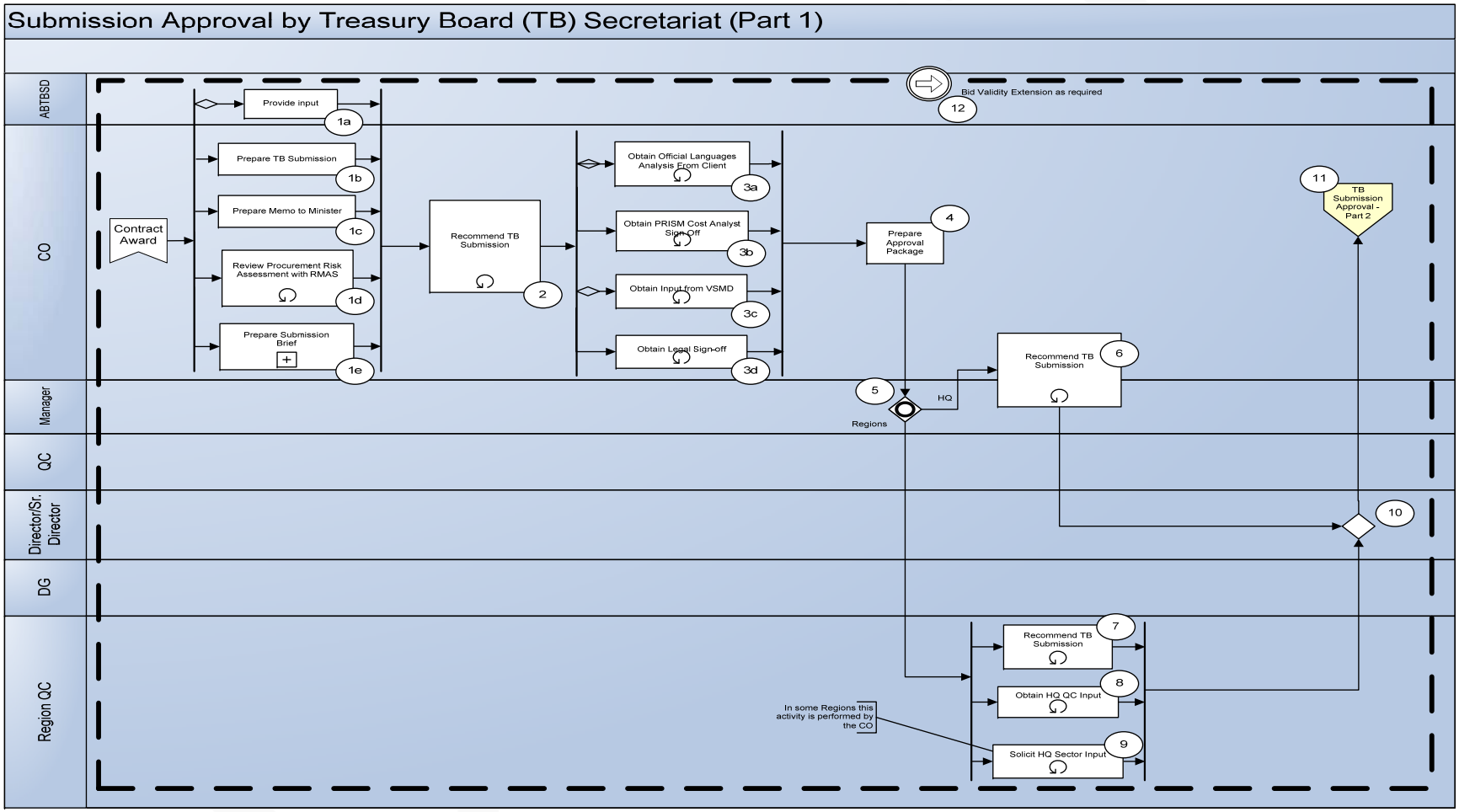


Figure 23 - Level 3 TB Submission Approval (Part 1) Business Process Model

Process Description

TB Submission Approval Part 1	
Summary Description	The purpose of this process is to obtain Treasury Board (TB) approval of a Treasury Board (TB) submission. This sub-process is covered in four parts. This first part of the process includes steps to, • prepare the TB submission, submission brief and memo to the Minister as required, • review a procurement risk assessment • forward and recommend the TB submission for approval(s) • obtain official languages analysis • obtain cost analysis and • obtain legal sign-off
Process Narrative ***Actors:*** • ***ABTBSD*** • ***Contracting Officer*** • ***Team Leader*** • ***Manager*** • ***QC*** • ***Director/Senior Director*** • ***Director General (DG)*** • ***Region QC***	The following process flow narrative pertains to Figure 23 : 1. Using the EPS solution, : a. ABTBSD provides input to the TB submission, b. the CO prepares the submission c. the CO prepares the memo to the minister (as required) d. the CO reviews the procurement risk assessment with RMAS e. the CO prepares the submission brief 2. The CO forwards the TB submission to the Team Lead and the Manager. Both the Team Lead and the Manager will review and recommend the TB Submission 3. The CO will then, a. obtain official languages analysis from the Client/End User, b. obtain cost analysis from the PRISM c. obtain input to the submission from VSMD d. obtain submission sign-off from Legal 4. The CO prepares the approval package 5. The manager at HQ or in the region submits the submission to the QC, Director/Senior Director, the DG and the regional QCfor recommendation. 6. The QC, Director/Senior Director and the DG recommend the submission 7. The regional QC recommends the submission 8. The regional QC obtains HQ QC input 9. The regional QC or CO obtains HQ sector input 10. Throughout the process, Bid Validity Extension may be required 11. The process proceeds to TB Submission (Part 2) 12. As required throughout the process, bid validity extensions may occur.

Input	Description
Request to Prepare TB Submission	A request is made to begin the TB Submission.
Output	**Description**
Recommended Draft TB Submission	A recommended Draft TB Submission is sent to the CO with specific guidelines.

Business Rules

The Treasury Board (TB) Submission approval business process is governed by the following rules:

1. Treasury Board approval guidelines available on the TBS web site
2. The TB submission approval process can be lengthy (e.g. 6 to 12 months)

b. TB Submission Approval (Part 2)

Process Model

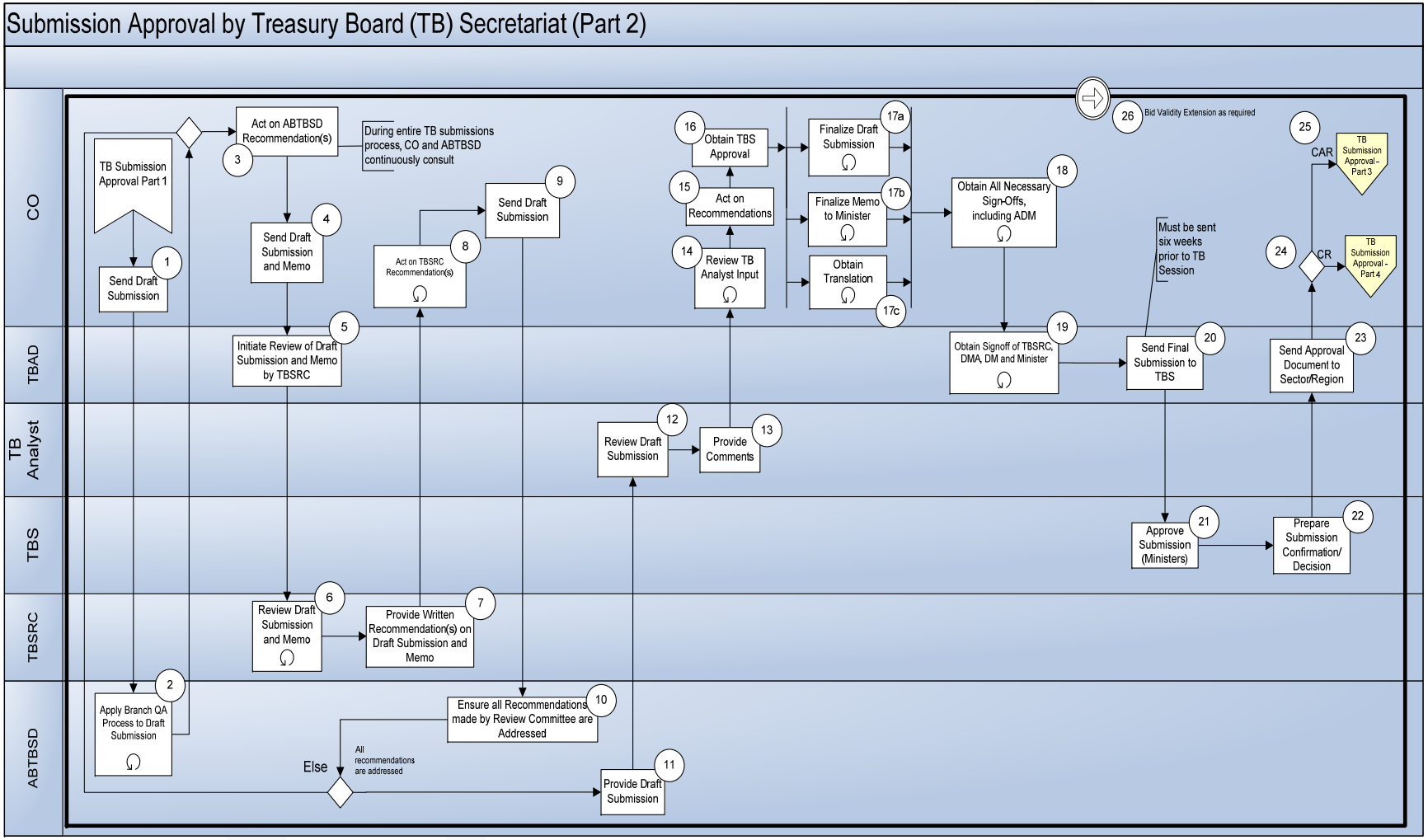


Figure 24 - Level 3 TB Submission Approval (Part 2) Business Process Model

Process Description

TB Submission Approval Part 2	
Summary Description	The purpose of this process is to obtain Treasury Board (TB) approval of a Treasury Board (TB) submission. This sub-process is covered in four parts. This second part of the process includes steps to, • forward the TB submission to various parties within TBS as required, • review & QA the submission by various parties within TBS as required, • forward and recommend the TB submission for approval(s) • finalize the TB submission, submission brief and memo to the Minister as required • obtain translation as required • obtain all necessary approvals & sign-off as required • obtain an approved document
Process Narrative ***Actors:*** • ***ABTBSD*** • ***Contracting Officer*** • ***TBAD*** • ***TB Analyst*** • ***TBS*** • ***TBSRC***	The following process flow narrative pertains to Figure 24 : Using the EPS solution 1. After receiving the draft submission, the CO forwards the draft submission to ABTBSD for branch QA 2. ABTBSD will QA the draft submission document and forward it back to the CO, 3. The CO will act on ABTBSD recommendations from their QA activity 4. The CO forwards the draft submission along with a memo to TBAD for review 5. TBAD will forward the draft submission and memo to TBSRC for review 6. TBSRC will review the draft submission 7. TBSRC will provide to the CO written recommendations on the draft submission 8. The CO will act on TBSRC recommendations 9. The CO forwards the draft submission along to ABTBSD for review 10. ABTBSD reviews the submission to ensure that all TBSRC recommendations have been addressed. The submission is returned to the CO if any recommendations are not addressed. 11. Once TBSRC recommendations have been addressed, they forward the submission to a TB analyst for input and review 12. The TB analyst reviews the submission 13. The TB analyst provides input and forwards the submission to the CO 14. The CO reviews the TB analyst's input to the submission 15. The CO will act on the TB analyst's recommendations from their review 16. The CO will obtain TBS approval on the revised submission 17. The CO will, a. finalize the draft submission, b. finalize the memo to the minister

	c. obtain translation of the submission and the memo (as required) 18. The CO will obtain all necessary sign-offs from all required parties including from the ADM and forwards the document to TBAD 19. TBAD obtains sign-off from TBSRC, the DMA, the DM and the Minister 20. TBAD forwards the final submission to TBS 21. TBS obtains Ministerial approval of the submission 22. TBS prepares a submission confirmation/decision and forwards the approval document to TBAD (as required) 23. TBAD forwards the approved submission and confirmation/decision to the sector/region (as required) 24. The process proceeds to TB Submission part four 25. The process proceeds to TB Submission part three 26. As required throughout the process, bid validity extensions may occur.

Input	Description
Draft TB Submission	A draft TB Submission is received by the CO.
Output	**Description**
Final Approved TB Submission	A final approved version of the TB Submission is completed.

Business Rules

The Treasury Board (TB) Submission approval business process is governed by the following rules:

1. Treasury Board approval guidelines available on the TBS web site
2. The TB submission approval process can be lengthy (e.g. 6 to 12 months)

c. TB Submission Approval (Part 3)

Process Model

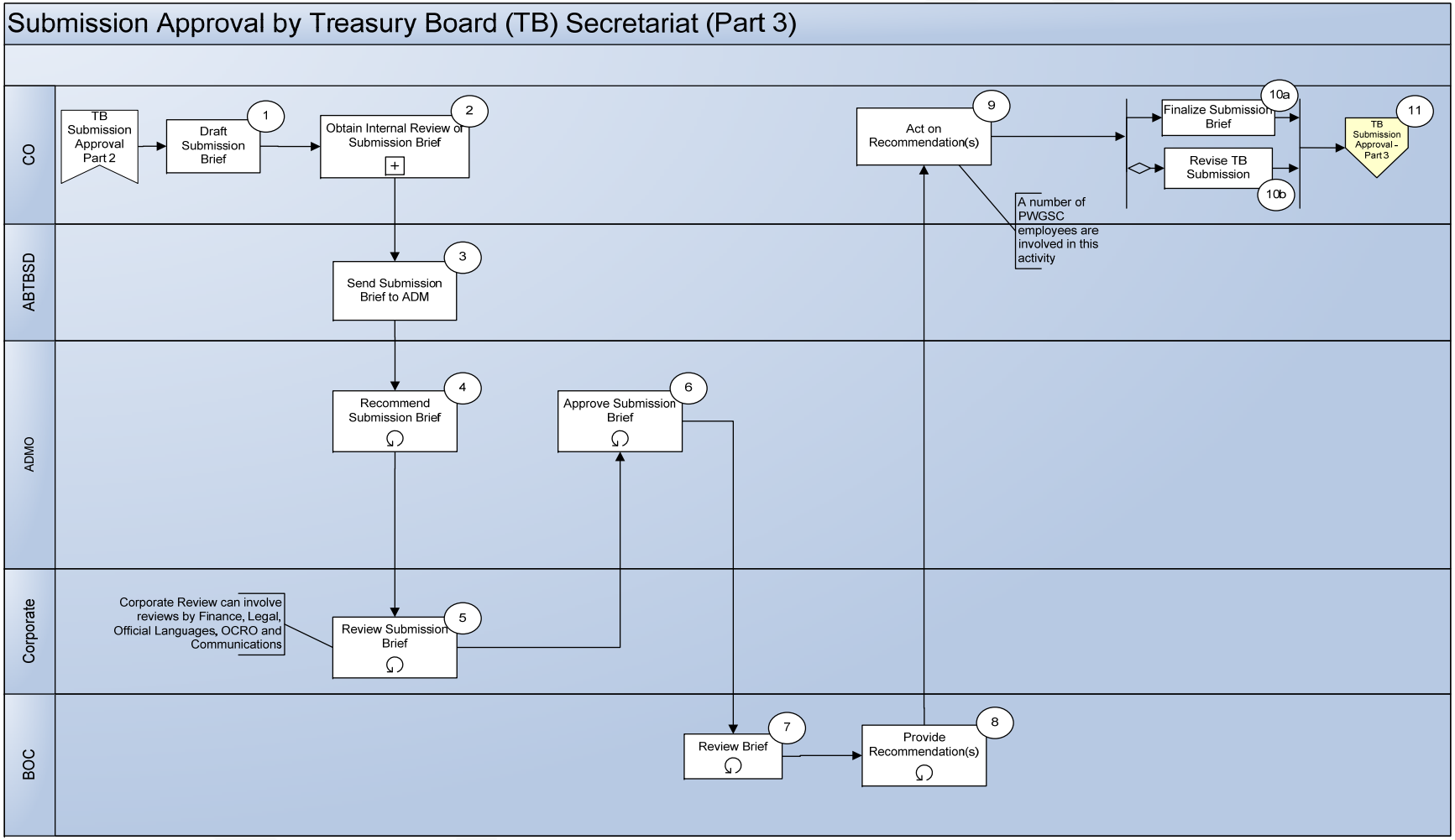


Figure 25 - Level 3 TB Submission Approval (Part 3) Business Process Model

Process Description

TB Submission Approval Part 3	
Summary Description	The purpose of this process is to obtain Treasury Board (TB) approval of a Treasury Board (TB) submission. This sub-process is covered in four parts. This third part of the process includes steps to, • draft, review, approve and finalize a submission brief with various parties
Process Narrative ***Actors:*** • ***ABTBSD*** • ***Contracting Officer*** • ***ADMO*** • ***Corporate*** • ***BOC***	The following process flow narrative pertains to Figure 25: Using the EPS solution 1. After completing the final submission, the CO drafts a submission brief for internal review 2. The CO obtains an internal review of the draft submission brief document and forwards it to ABTBSD, 3. ABTBSD forwards the draft submission brief document to the ADMO 4. The ADMO recommends the draft submission brief and forwards it to Corporate for their review 5. Corporate reviews the brief and returns it to the ADMO for approval. This corporate review can include Finance, Legal, Official Languages, OCRO and Communications. 6. The ADMO approves the submission brief and forwards the approved brief to BOC 7. BOC reviews the brief 8. BOC provides recommendations and forwards the brief along with their recommendations to the CO 9. The CO acts on BOC recommendations 10. The CO will, a. Finalize the submission brief and b. Revise the TB submission as required 11. The process proceeds to TB Submission part four

Input	Description
Draft TB Submission Brief	A draft TB Submission Brief is created.
Output	**Description**
Final Approved Draft TB Submission Brief	Final Draft TB Submission Brief is approved and attached with the Draft TB Submission.
Revised TB Submission	Both the submission and brief are compiled into one package.

Business Rules

The Treasury Board (TB) Submission approval business process is governed by the following rules:

1. Treasury Board approval guidelines available on the TBS web site
2. The TB submission approval process can be lengthy (e.g. 6 to 12 months)

d. TB Submission Approval (Part 4)

Process Model

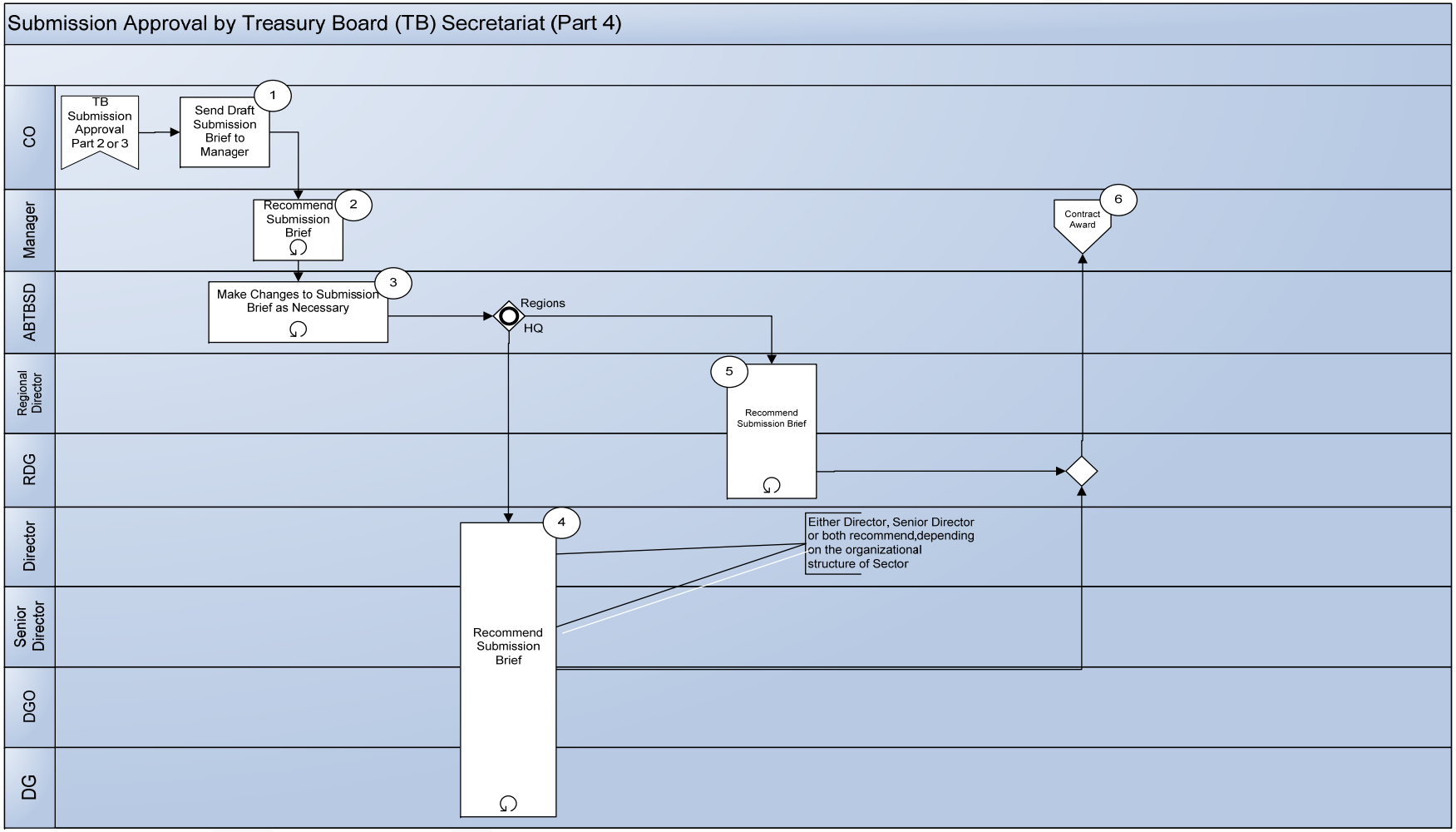


Figure 26 - Level 3 TB Submission Approval (Part 4) Business Process Model

Process Description

TB Submission Approval Part 4	
Summary Description	The purpose of this process is to obtain Treasury Board (TB) approval of a Treasury Board (TB) submission. This sub-process is covered in four parts. This fourth part of the process includes steps to, • obtain approval of a final submission brief from various parties
Process Narrative ***Actors:*** • ***ABTBSD*** • ***Contracting Officer*** • ***Manager*** • ***DGO*** • ***Regional Director*** • ***Senior Director*** • ***Director General (DG)*** • ***Regional DG (RDG)***	The following process flow narrative pertains to Figure 26: Using the EPS solution 1. After completing the draft submission brief, the CO forwards the brief their manager 2. The CO's manager reviews and recommends the draft submission brief document and forwards it to ABTBSD 3. ABTBSD makes all necessary changes to the brief and forwards it to one or both of senior management within HQ or the regions as required 4. Senior management within HQ, specifically the Director, Senior Director, DGO and the DG review and recommend the brief 5. Senior management within the regions, specifically the Regional Director, and the Regional DG review and recommend the brief 6. The process of TB Submission part four ends and returns to Contract Award.

Input	Description
Final Approved Draft TB Submission Brief	Final version of the Draft TB Submission Brief is approved.
Output	**Description**
Final Approved TB Submission Brief	Final version of the Draft TB Submission Brief is approved and is sent to Contract Award documentation.

Business Rules

The Treasury Board (TB) Submission approval business process is governed by the following rules:

1. Treasury Board approval guidelines available on the TBS web site
2. The TB submission approval process can be lengthy (e.g. 6 to 12 months)

8.3 Level 1 Business Process Models and Descriptions

a. Supplier Relationship Management (SRM)

Process Model

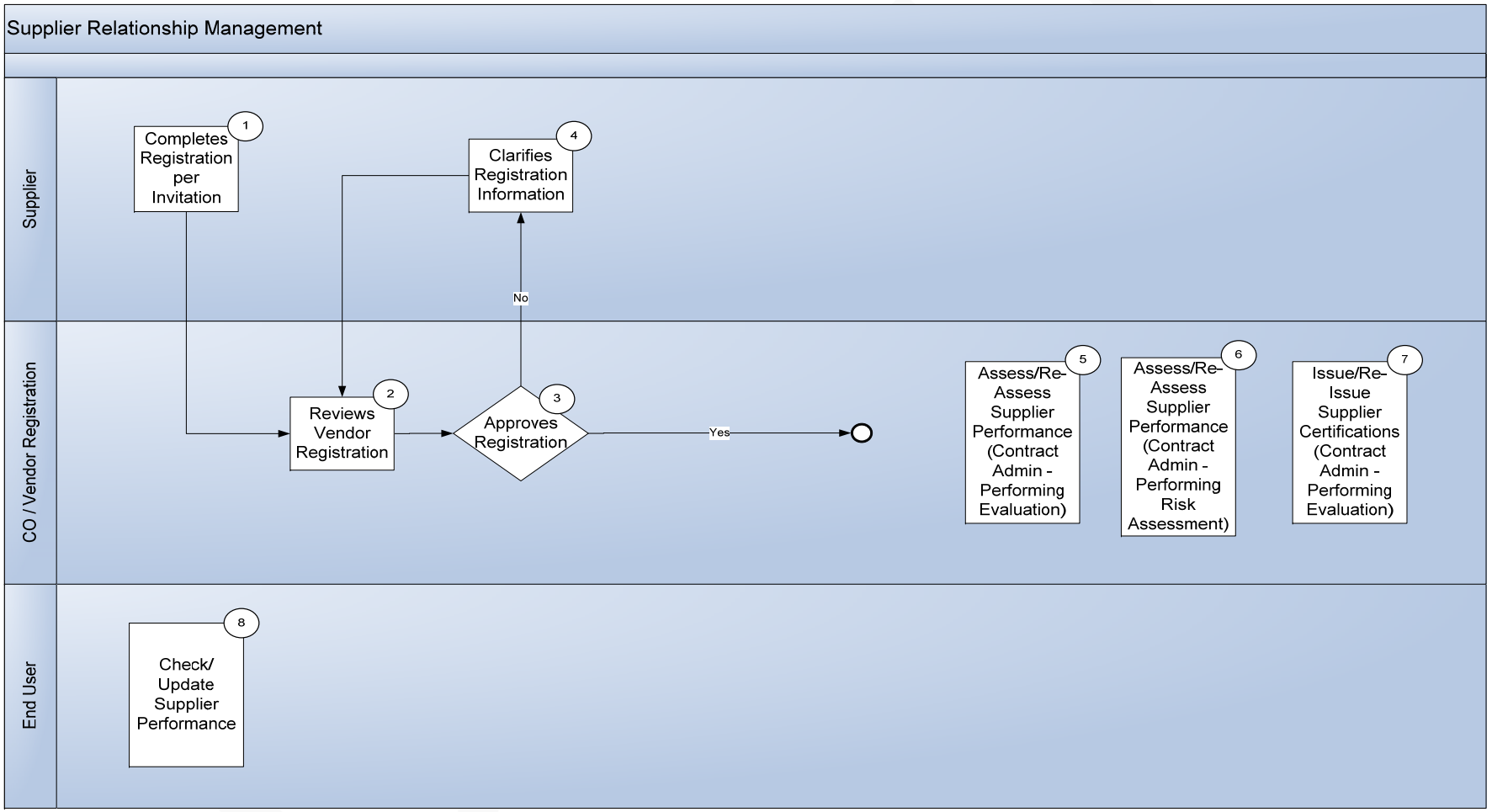


Figure 27 - Level 1 Supplier Relationship Management (SRM) Business Process Model

Process Description

Supplier Relationship Management	
Summary Description	The purpose of this Supplier Relationship Management (SRM) process is to manage the relationship with suppliers by, • providing the ability to register suppliers as well as a supplier on-boarding or self-registration process, • recording, tracking and managing supplier performance, qualifications, certification and accreditation • assessing, recording, tracking and managing operational supply risk This process includes the following steps: • supplier registration • assessing/re-assessing supplier performance and risk • verifying supplier performance via a catalogue purchase or the procurement sourcing cycle • issue/revoke/re-issue supplier accreditations and/or certifications
Process Narrative ***Actors:*** • ***End-User. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Supplier***	The following process flow narrative pertains to Figure 27 : Using the EPS solution, 1. The Supplier completes their registration as per the instructions in the received invitation to register 2. The CO reviews the registration and requests any corrections from the Supplier before approving the registration 3. The registration requires CO approval 4. If the registration information requires clarification, the Supplier clarifies any required information. Once the registration is approved the Supplier receives confirmation and the process ends. 5. The CO will need to Assess or Re-Assess Supplier Performance when conducting the Contract Administration task of Conducting a Supplier Performance Evaluation. 6. The CO will need to Assess or Re-Assess Supplier Performance when conducting the Contract Administration task of Conducting a Supplier Risk Assessment. 7. When performing the Contract Administration task of Conducting a Supplier Performance Evaluation, the CO can Issue or Re-Issue Supplier Certification to the Supplier for confirmation of certification 8. The Client (End User) or CO may need to Check Supplier Performance during either a catalogue purchase or a sourced procurement during the “Contract Award” process.

Input	Description
Supplier Registration Information	Supplier Registration Information provided by Suppliers, COs & End Users
Output	**Description**

New/Updated Supplier Registration Information	New/updated Supplier registration Information provided by Suppliers, COs & End Users
New/Updated Supplier Certification Information	New/updated Supplier certification information provided by Suppliers, COs & End Users

Business Rules

The Supplier Relationship Management business process is governed by the following rules:

1. N/A

b. Supplier Bid Submission

Process Model

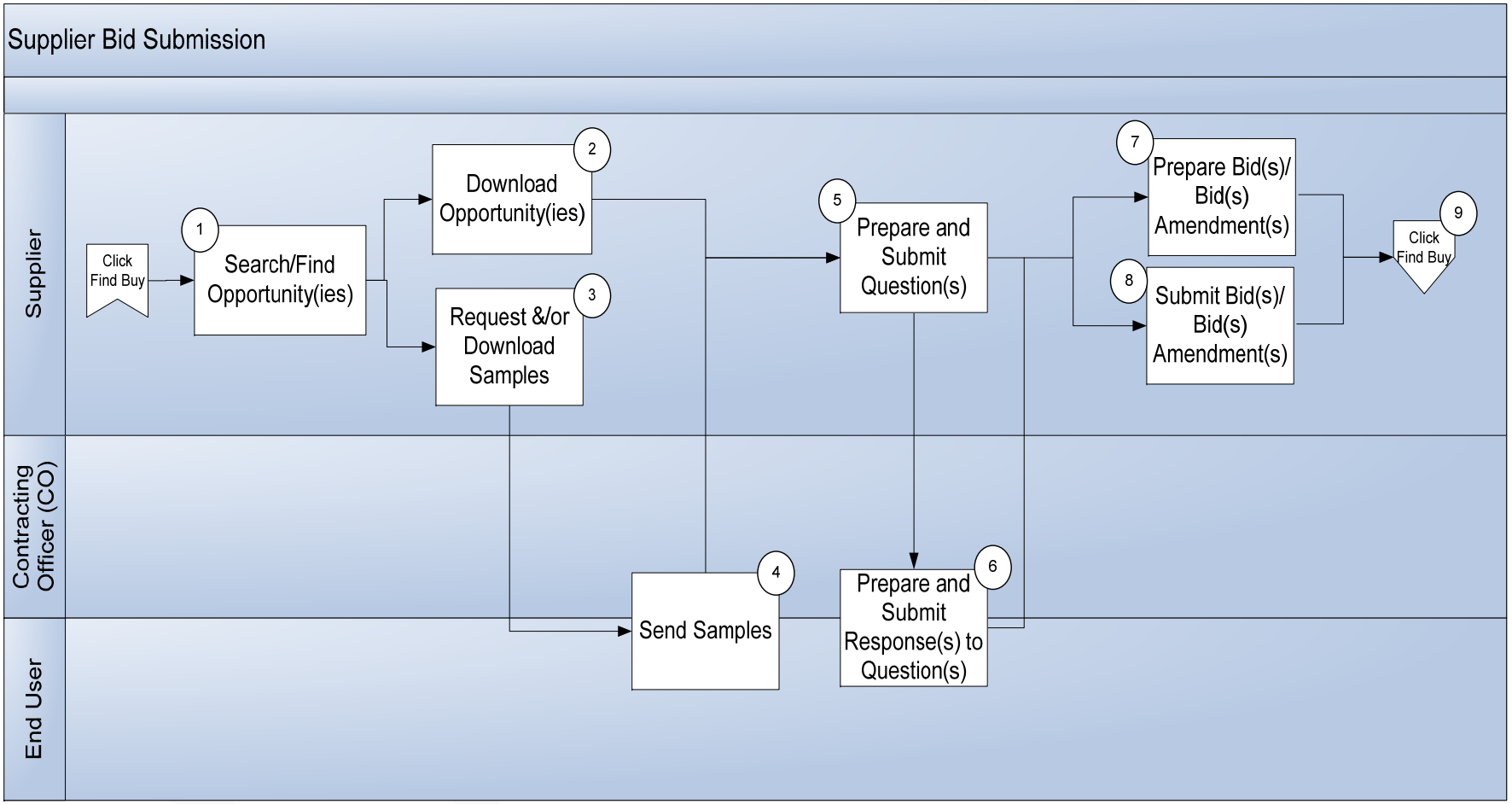


Figure 28 - Level 1 Supplier Bid Submission Business Process Model

Process Description

Supplier Bid Submission	
Summary Description	The purpose of this Supplier Bid Submission process is to provide to suppliers the ability to submit bids electronically using EPS by, • searching for opportunities on GETS, • downloading solicitation documents and samples from GETS • submit samples, bids and responses to questions
Process Narrative ***Actors:*** • ***End-User. The End User is either the Proxy Requester or Client Requester*** • ***Contracting Officer*** • ***Supplier***	The following process flow narrative pertains to Figure 28 : Using the EPS solution, 1. The Supplier(s) searches for various opportunities on GETS. 2. the Supplier (s) downloads solicitation documents as required 3. the Supplier (s) downloads samples as required 4. the Supplier uploads or submits samples sample(s) for the CO & End User as required 5. the Supplier may prepare and submit/upload question(s) if and as required 6. the CO and End User will then prepare and submit/upload response(s) to Supplier questions as required 7. the Supplier will then prepare bid(s) or bid(s) amendment(s) if and as required 8. the Supplier will then submit/upload bid(s) or bid(s) amendment(s) if and as required 9. the process returns to Click Find Buy

Input	Description
Supplier Has Logged Into the Portal	Supplier logs into the Portal.
Output	**Description**
Solicitation Documents/Samples	Solicitation documentation and/or samples are viewable in the Portal.
Responses to Questions	Supplier responds to questions from CO and/or End User.
Bid Submissions	Supplier receives bid submissions.

Business Rules

The Supplier Bid Submission business process is governed by the following rules:

1. N/A

ATTACHMENT 1 TO PART 4:

EVALUATION AND SELECTION METHODOLOGY

Table of Contents

1. Overview of this Attachment

This Attachment outlines the evaluation methodology and the basis of selection to be used in the evaluation of proposals received in response to this RFP. The evaluation methodology and basis of selection are structured to ensure a fair and consistent assessment of the solutions proposed by Bidders.

2. Evaluation Methodology

The Bidder whose proposal receives the highest combined rating of technical merit and price (adding the Technical Proposal – Rated Requirements score, the Technical Proposal – Usability Assessment score and the Financial Proposal score) will be recommended for award of a Contract.

3. Evaluation Weighting

Evaluation Element	Proposal Element	Weight
Technical Score	Technical Proposal – Rated Requirements	600 points
	Technical Proposal – Usability Assessment	100 points
Financial Score	Financial Proposal	300 points
	TOTAL	1000 points

4. Evaluation Process

The e-Procurement Solution (EPS) proposal evaluation team will conduct the evaluation of the proposals as follows:

(1) Proposals will be assessed for their compliance with the Mandatory Requirements identified in this Solicitation, including but not limited to the Supply Chain Security Information assessment, the Financial Capability assessment and all Certifications as described in Part 5. Failure to meet any mandatory requirements of the Solicitation will result in the proposal being deemed non-responsive and it will be given no further consideration. Responsive proposals which have completed this step will be assessed under Step (2).

(2) Proposals deemed responsive to the requirements of Step (1) will be assessed against the technical Mandatory Requirements identified in Attachment 2 to Part 4 – Technical Evaluation. Proposals not complying with all Mandatory Requirements identified in Attachment 2 to Part 4 – Technical Evaluation will be deemed non-responsive and will receive no further consideration. Responsive proposals which have completed this step will be assessed under Step (3).

(3) Proposals deemed responsive to the requirements of Step (2) will be assessed against the technical Point Rated Requirements identified in Attachment 2 to Part 4 – Technical Evaluation. To be deemed responsive to the technical Point Rated Requirements, it is mandatory that all pass marks as identified in Attachment 2 to Part 4 – Technical Evaluation be met including the overall minimum pass mark. To be thorough, Canada will continue to evaluate a proposal even if it fails a single pass mark, however, Canada may stop evaluating a proposal where it has failed three pass marks. Proposals not passing all of the pass marks will be deemed non-responsive. Proposals deemed non-responsive will be given no further consideration. Responsive proposals which have completed this step will be assessed under Step (4).

(4) The Usability Assessment identified in Attachment 3 to Part 4 – Usability Assessment will be assessed for each responsive proposal and a score assigned from the points available for this element. There is no pass mark for the Usability Assessment. Responsive proposals which have completed this step will be assessed under Step (5).

(5) The Financial Proposals of responsive bids will be evaluated by the Contracting Authority and financial points will be assessed in accordance with section 6. *Financial Evaluation* of this Attachment. Only the top ranked responsive proposal following the evaluation of the Technical and Financial Proposals will proceed to Step (6). All other proposals will be given no further consideration.

(6) A Proof of Proposal (PoP) test may be conducted on the highest ranked proposal by PWGSC to confirm the authenticity of the proposed solution. The proposal will be evaluated for its compliance with all requirements of the PoP test. If the proposal does not comply with all requirements of the PoP test, the Bidder will be given 5 working days, or a longer period if specified in writing by the Contracting Authority, to correct the areas of non-compliance in its solution before the areas of non-compliance are tested once again. If the proposal is compliant with all requirements of the PoP test, the Bidder will be recommended for Contract Award. If the proposal still does not comply with all requirements of the PoP test after the second test is administered, it will be deemed non-responsive and given no further consideration. Canada will then proceed with Step (6) for the next highest ranked responsive proposal as determined in Step (5).

Canada reserves the right to conduct any step in the evaluation process concurrently or out of sequence.

Proposals will be evaluated individually in accordance with this RFP and its Annexes, Appendices, Attachments, and Forms.

Bidder's information required to evaluate proposals must not be provided through references to web sites. Any such information must be provided with the Bidder's proposal. Canada will not consider information that is solely provided though references to web sites.

5. Technical Evaluation

The Technical Evaluation includes the Mandatory Requirements, the Rated Requirements and the Usability Assessment.

5.1 Mandatory Requirements

Proposals will first be assessed for their compliance with the Mandatory Requirements identified in this Solicitation, including but not limited to the Supply Chain Security Information assessment, the Financial Capability assessment and all Certifications as described in Part 5 of the RFP. Proposals will then be assessed for their compliance with the Mandatory Requirements identified in Attachment 2 to Part 4 – Technical Evaluation.

Bidders must meet all of the mandatory requirements in order to be considered responsive. Failure to meet any mandatory requirement will result in the proposal being deemed non-responsive and it will be excluded from further consideration.

5.2 Rated Requirements

Each proposal will be rated by assessing a score, rounded to two decimal points, to each rated requirement as identified in Attachment 2 to Part 4 – Technical Evaluation. The degree of importance of each Rated Requirement is determined by the points allocated to each criterion.

To be deemed responsive to this element of the evaluation, it is mandatory that all pass marks as identified in Attachment 2 to Part 4 – Technical Evaluation be met including the overall minimum pass mark.

5.2.1 Process

a. An evaluation team composed of representatives of Canada will evaluate the proposals on behalf of Canada. Canada may hire any independent consultant or use any Government resources to evaluate any proposal. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

b. Canada has engaged a Fairness Monitor for this procurement. The Fairness Monitor will not be part of the evaluation team, but will observe the evaluation of the proposals with respect to Canada's adherence to the evaluation process described in this Solicitation.

c. A consensus process through both written and oral evaluations will be used to arrive at a consensus score for each criterion being evaluated.

d. The evaluation team are considered the scoring members. Non-scoring members such as subject matter experts are not allowed to score, but they may provide comments, if requested to do so, during the development of a consensus score. These comments are taken into account by the evaluation team during consensus deliberations.

e. At the consensus meetings, individual scores are presented and a consensus discussion follows to consider each of the individual score positions to arrive at an overall consensus score.

f. During consensus, it may be necessary to contact the reference(s) for verification or validation of what the Bidder has proposed in its proposal. Refer to section *4.7 Reference Checks* of this Solicitation for further details on the Reference Checks process.

5.3 Usability Assessment

Each Usability Assessment will be evaluated by assessing a score, rounded to two decimal points, to each usability scenario, as identified in Attachment 3 to Part 4 – Usability Assessment.

5.4 Total Technical Score

The Total Technical Score will be calculated by adding the points for Technical Evaluation – Rated Requirements and Technical Evaluation – Usability Assessment.

6. Financial Evaluation

The points for the Financial Evaluation will be allocated as follows:

6.1 Financial Score

6.1.1 Financial Proposals

All proposals that have met all mandatory requirements of this Solicitation and that have been deemed technically responsive will have its proposed fees evaluated in accordance with the following.

6.1.2 Calculation of the Total Evaluated Proposal Price

The Total Evaluated Proposal Price will be calculated as follows, rounded to two decimal points, using the fees as calculated in Attachment 5 to Part 4 – Financial Evaluation, Customs duties are included and Applicable Taxes are extra:

Item	Applicable Fee	Subtotal
1	EPS Transition-In Fee	
2	EPS Operational Fee – Tier 1: 1 to 5,000 Users	
3	EPS Operational Fee – Tier 2: in excess of 5,000 Users	
4	EPS Operational Fee – Tier 3: Unlimited Users	
5	Optional Work – Fixed Prices	
6	Professional Services	
Total Evaluated Proposal Price (sum of the subtotals for items 1 through 6)		

6.1.3 Evaluation of Fees

a. The Total Evaluated Proposal Price for each responsive Bidder will be added together and divided by the number of responsive Bidders to calculate the average (Mean Amount).

b. Firstly, a Normalized Raw Score will be determined, rounded to three decimal points, by application of the following formula:

Normalized Raw Score = 1 – Absolute value of ((Mean Amount – Total Evaluated Proposal Price) ÷ Mean Amount)

OR

= 1 – |(Mean Amount – Total Evaluated Proposal Price) ÷ Mean Amount|

c. The Normalized Raw Score measures the Bidder's Total Evaluated Proposal Price against the average of all Bidders' Total Evaluated Proposal Price.

d. Secondly, a Correction Factor will be used, rounded to three decimal points, to favour lower total proposal prices:

All responsive proposals will be ranked, and:

the Bidder with the lowest Total Evaluated Proposal Price will receive 100% of its Normalized Raw Score;
the Bidder with the lowest Total Evaluated Proposal Price will receive 80% of its Normalized Raw Score;
the Bidder with the lowest Total Evaluated Proposal Price will receive 60% of its Normalized Raw Score;
the Bidder with the lowest Total Evaluated Proposal Price will receive 40% of its Normalized Raw Score;
the Bidder with the lowest Total Evaluated Proposal Price will receive 20% of its Normalized Raw Score; and
all other bidders will receive 10% of their Normalized Raw Score.

e. Lastly, points will be assigned, rounded to two decimal points, based on the following formula:

Score = Normalized Raw Score X Correction Factor X 30% X 1000

Example

Example of 4 proposals received in response to this RFP (numbers are only for illustrative purposes):

Bidder A:

Item	Applicable Fee	Subtotal
1	EPS Transition-In Fee	$5,000,000
2	EPS Operational Fee – Tier 1: 1 to 5,000 Users	$2,500,000
3	EPS Operational Fee – Tier 2: in excess of 5,000 Users	$1,000,000
4	EPS Operational Fee – Tier 3: Unlimited Users	$5,000,000
5	Optional Work – Fixed Prices	$500,000
6	Professional Services	$1,000,000
Total Evaluated Proposal Price (adding subtotals for items 1 through 6)		$15,000,000

Bidder B:

Item	Applicable Fee	Subtotal
1	EPS Transition-In Fee	$2,000,000
2	EPS Operational Fee – Tier 1: 1 to 5,000 Users	$3,500,000
3	EPS Operational Fee – Tier 2: in excess of 5,000 Users	$1,500,000
4	EPS Operational Fee – Tier 3: Unlimited Users	$8,000,000
5	Optional Work – Fixed Prices	$800,000
6	Professional Services	$1,200,000
Total Evaluated Proposal Price (adding subtotals for items 1 through 6)		$17,000,000

Bidder C:

Item	Applicable Fee	Subtotal
1	EPS Transition-In Fee	$2,500,000
2	EPS Operational Fee – Tier 1: 1 to 5,000 Users	$1,500,000
3	EPS Operational Fee – Tier 2: in excess of 5,000 Users	$1,000,000
4	EPS Operational Fee – Tier 3: Unlimited Users	$4,000,000
5	Optional Work – Fixed Prices	$500,000
6	Professional Services	$500,000
Total Evaluated Proposal Price (adding subtotals for items 1 through 6)		$10,000,000

Bidder D:

Item	Applicable Fee	Subtotal
1	EPS Transition-In Fee	$5,000,000
2	EPS Operational Fee – Tier 1: 1 to 5,000 Users	$4,500,000
3	EPS Operational Fee – Tier 2: in excess of 5,000 Users	$3,000,000
4	EPS Operational Fee – Tier 3: Unlimited Users	$12,000,000
5	Optional Work – Fixed Prices	$3,000,000
6	Professional Services	$2,500,000
Total Evaluated Proposal Price (adding subtotals for items 1 through 6)		$30,000,000

Results:

	Total Fees	Deviation	Normalized Raw Score	Rank	Correction (%)	Score (out of 300)
Bidder A	$15,000,000	$(3,000,000)	0.833	2	80%	199.80
Bidder B	$17,000,000	$(1,000,000)	0.944	3	60%	169.80
Bidder C	$10,000,000	$(8,000,000)	0.556	1	100%	166.80
Bidder D	$30,000,000	$12,000,000	0.333	4	40%	39.90
Total all Proposals				$76,000,000		
Average (Mean)				$18,000,000		
Number of Bidders				4		
Standard Deviation				1		

6.1.4 Scoring for Only Two Proposals

In the event that only two proposals are deemed responsive to the requirements of the RFP (including the Mandatory and Point Rated technical evaluation criteria), the calculations for the scores will be as follows:

The proposal with the lowest Total Evaluated Proposal Price will be awarded 300 points. The remaining proposal will have its Total Evaluated Proposal Price prorated against the lowest Total Evaluated Proposal Price, rounded to two decimal points. The following formula will be applied:

Financial Score = (Lowest Total Evaluated Proposal Price / Bidder's Total Evaluated Proposal Price) * 300

Example

Example of 2 proposals received in response to this RFP (numbers are only for illustrative purposes):

Bidder	Total Evaluated Proposal Price	Financial Score
Bidder A	$18,000,000	($16,000,000/$18,000,000) * 300 = 267.00
Bidder B	$16,000,000	($16,000,000/$16,000,000) * 300 = 300.00

7. Basis of Selection

The Bidder whose proposal receives the highest combined rating of technical merit and price (adding the Technical Proposal – Rated Requirements score, the Technical Proposal – Usability Assessment score and the Financial Proposal score), will be considered as representing best value to Canada and will be recommended for award of a Contract.

If more than one Bidder is tied for the highest Total Score, the responsive proposal with the highest Total Technical Score will be recommended for award of a Contract.

Example

Bidder	Rated Requirements Score	Usability Assessment Score	Total Technical Score (A)	Financial Score (B)	Total Score (A) + (B)
Bidder A	495.00	75.00	570.00	199.80	769.80
Bidder B	550.00	95.00	645.00	169.80	814.80
Bidder C	465.00	80.00	545.00	166.80	711.80
Bidder D	580.00	85.00	665.00	39.80	704.80

In the example above, Bidder B would be recommended for Contract award.

ATTACHMENT 2 TO PART 4:

TECHNICAL EVALUATION

TABLE OF CONTENTS

1. Evaluation Summary

Technical Evaluation					
No.	**Mandatory Criteria**			**Compliant / Non-Compliant**	
M1	Solution Management Services				
M2	Data Residency				
No.	**Point-Rated Criteria**	**Scale[1]**	**Maximum Points**	**Maximum Points**	**Pass Mark**
R1	**Corporate Experience**			**60**	**36**
R1.1	Solution Management Services – Additional	1	54		
R1.2	SAP Certified Partner Solution	*	6		
R2	**Implementation Plan**			**120**	**72**
R2.1	Project Implementation Plan	2	62.4		
R2.2	Training Plan	2	33.6		
R2.3	Change Management and Communication Plan	2	24		
R3	**Management Approach**			**150**	**90**
R3.1	Organizational Structure and Use	2	24		
R3.2	Risk Management	2	24		
R3.3	Relationship Management	2	24		
R3.4	Service Desk Support	2	30		
R3.5	Value Added	2	30		
R3.6	Product Roadmap	2	18		
R4	**Technical Approach**			**90**	**54**
R4.1	Technical Deployment Model - SaaS	2	30		
R4.2	Technical Architecture	2	30		
R4.3	Technical Integration	2	15		
R4.4	IT Service Continuity Plan	2	15		
R5	**Security Plan**			**90**	**63**
R5.1	Policies and Procedures (Controls)	2	9		

R5.2	IT Security Topology Diagram	2	6		
R5.3	Forensic Procedures and Safeguards	2	12		
R5.4	Security Organization	2	9		
R5.5	Data Segregation	2	12		
R5.6	Disposal	2	9		
R5.7	Continuous Monitoring Program Services	2	13.5		
R5.8	Industry IT Security Certifications	2	6		
R5.9	Identity, Credential and Access Management	*	13.5		
R6	**Additional Functional Requirements**			**90**	**45**
R6.1	General	*	2.7		
R6.2	Sourcing and Contract Management	*	21.6		
R6.3	Procurement Management	*	11.7		
R6.4	Service Procurement	*	26		
R6.5	Business Intelligence	*	6		
R6.6	Supplier Relationship Management	*	22		
	Overall Maximum Points & Pass Threshold:			**600**	**360**

Notes:
[1]Please refer to the Technical Evaluation Scales included at section 4 of this attachment.
*The above noted criteria do not use a scale. These criteria have points assigned to specific elements.

2. Mandatory Criteria

No.	Evaluation Area	Bid Submission Requirements	Evaluation Criteria	Applicable Scale
M1	EPS Management Services	The Bidder must clearly demonstrate its experience in the provision of services of similar nature and scope as the services described in this Solicitation by providing the following for 1 project where it provided an e-procurement solution for a client that is arms-length from the Bidder and not an affiliate of the Bidder: i. a description of the project; ii. the period during which the e-procurement solution was operational; iii. the number of internal users; iv. the value of the Orders, in a 12 consecutive month period, that were processed in the e-procurement solution through services similar in nature and scope to the services described in the Procurement Management section of the Statement of Work (SOW); v. the number of Contracts, in a 12 consecutive month period, that were awarded in the e-procurement solution through services similar in nature and scope to the services described in the Sourcing and Contract Management section of the SOW;	The Bidder must clearly demonstrate its experience in the provision of an e-procurement solution of similar nature and scope to at least the following sections as described in Part 5 of the SOW: o 5.3 Section A: General Requirements - Workflow; o 5.5 Section C: Sourcing and Contract Management; o 5.6 Section D: Procurement Management; o 5.10 Section H: Supplier Relationship Management; and o 5.12 Section J: User Management. The Bidder must have provided an e-procurement solution on a project for a client that is arms-length from the Bidder and not an affiliate of the Bidder, whereby: (a) the Bidder delivered or was responsible for the management of a web-enabled e-procurement solution; (b) the e-procurement solution must have been operational (in production) for a minimum of a 12 consecutive month period;	Compliant / Non-Compliant

		vi. a description of the e-procurement solution software functionalities that were implemented; vii. the client business name; and viii. the client point of contact, including full name, phone number and email address.	(c) the e-procurement solution must have had a minimum of 25,000 Internal Users with access to the production system; (d) a minimum of $1,000,000,000 (CAD, taxes extra), foreign currency will be based on the Bank of Canada daily noon exchange rate on January 15th, 2016) in Orders, in 12 consecutive month period, were processed in the e-procurement solution through services similar in nature and scope to the services described in the Procurement Management section of the SOW; and (e) a minimum of 10,000 Contracts, in a 12 consecutive month period, must have been awarded in the e-procurement solution through services similar in nature and scope to the services described in the Sourcing and Contract Management section of the SOW. The Bidder must have assumed the responsibility and liability for the provision of the services of the e-procurement solution. For the purpose of this criteria, internal users mean an individual who is employed by the client or a representative of the client.	

M2	Data Residency	The Bidder must clearly demonstrate its ability to comply with the requirements of this Solicitation placing restrictions on data residency to Canada or to countries with which Canada has international bilateral industrial security instruments (IBISI). The Bidder must clearly demonstrate its EPS data residency compliance by providing relevant data center certifications and its deployment plan which must include specifics on: i. location(s) of primary data center(s); ii. location(s) of secondary data center(s); iii. location(s) of all the infrastructure components (including, but not limited to, database servers, data, application servers); and iv. locations of the Security Operations Centre (SOC), Network Operations Centre (NOC) and the Service Desk. Canada currently has international bilateral industrial security instruments with the following countries: • Australia • Belgium • Denmark • Finland • France • Germany	The Bidder must demonstrate that the data residency for the entire EPS solution, the SOC, NOC and Service Desk and all personnel providing assistance and support as part of the SOC/NOC and Service Desk, resides in Canada and/or countries with which Canada has international bilateral industrial security instruments (IBISI).	

		• Israel • Italy • Netherlands • New Zealand • Norway • Spain • Sweden • Switzerland • The United Kingdom • The United States Furthermore, the Bidder must demonstrate that its SOC, its NOC and its Service Desk reside in one or more of the countries listed above. The bidder must also demonstrate that the personnel providing assistance and support as part of the SOC/NOC and Service Desk are also physically located in the countries listed above.		

3. Point-Rated Criteria

No.	Evaluation Area	Bid Submission Requirements	Evaluation Criteria
R1	**Corporate Experience**		
R1.1	EPS Management Services – Additional	The Bidder should submit descriptions of up to 5 web-enabled e-procurement solution projects which demonstrate the Bidder's experience in delivering services of similar nature and scopes as this Solicitation for clients that are arms-length from the Bidder and not an affiliate of the Bidder:, by providing the following for each project: i. a description of the project; ii. the period during which the e-procurement solution was operational; iii. the number of internal users; iv. the value of the Orders, in a 12 consecutive month period, that were processed in the e-procurement solution through services similar in nature and scope to the services described in the Procurement Management section of the SOW; v. the number of Contracts, in a 12 consecutive month period, that were awarded in the e-procurement solution through services similar in nature and scope to the services described in the Sourcing and Contract Management section of the SOW;	Canada will evaluate up to 5 e-procurement solution projects submitted by the Bidder for clients that are arms-length from the Bidder and not an affiliate of the Bidder and will evaluate the degree to which the Bidder demonstrates aggregate experience in successfully delivering services of similar nature and scope as this Solicitation and: (a) had 500,000 Internal Users with access to the production system of the e-procurement solution; (b) had $20,000,000,000 (CAD, taxes extra, foreign currency will be based on the Bank of Canada daily noon exchange rate on January 15th, 2016) in Orders, that in a one year period, that were processed in the e-procurement solution through services similar in nature and scope to the services described in the Procurement Management section of the SOW; and (c) had 250,000 Contracts must have been awarded in the e-procurement solution through services similar in nature and scope to the services described in the Sourcing and Contract Management section of the SOW In determining the Bidder's score, in addition to evaluating the aggregate experience of the Bidder's projects as

		vi. a description of the e-procurement solution software functionalities that were implemented; vii. the client business name; and viii. the client point of contact, including full name, phone number and email address. Each project should not exceed 10 pages in length. Where pages exceed this length, Canada will only review the first 10 pages in order of appearance in the bid. The up to 5 projects must not include the project the bidder submits on criteria M1. If so, that project will not be considered amongst the up to 5 projects requested in criteria R1.1.	identified above, Canada will evaluate the similarity and relevancy of the scope of the projects as follows: (a) the solution implemented is the same functional solution they are proposing in response to the Solicitation; (b) the time period that the solution was operational and being used by the client (start and end dates); (c) the solution implemented is still in use by the client (as of January 5, 2016) (d) the solution was implemented for a public sector client; (e) the solution was delivered as a managed service (f) the solution implemented integrated with the client's SAP Finance system; and (g) the types of services provided; (h) the degree to which the Bidder was successful at meeting the contracted timelines; (i) the degree to which the Bidder was successful at managing change requests; and (j) the degree to which the Bidder was successful at delivering on project results within budget. The bidder must have assumed the responsibility and liability for the provisions of the services of the e-procurement solution. If more than five (5) projects are proposed, only the first five (5) projects in the order of presentation will be evaluated.

			The up to 5 projects must not include the project the bidder submits on criteria M1. If so, that project will not be considered amongst the up to 5 projects requested in criteria R1.1.
R1.2	SAP Certified Partner Solution	The Bidder should provide copies of the following certifications: i. for the Bidder, an SAP Certified Partner certification; and ii. for the Bidder's EPS software, an SAP Certified Partner Solution certification.	Canada will evaluate based on the following: (a) the Bidder is an SAP Certified Partner = 3 points (b) the EPS proposed by the Bidder is an SAP Certified Partner Solution = 3 points Maximum of 6 point.
R2	**Implementation Plan**		
R2.1	Project Implementation	The Bidder should describe its proposed approach to the EPS implementation that describes the Bidder's approach to meet the requirements of this Solicitation, including implementation of the complete EPS and transformation of the GC procurement process, including: i. a description of each of the major tasks required to implement the EPS and what each of the tasks will accomplish. The Bidder should add as many subtasks as necessary to describe all the major tasks. The tasks described in this subsection are not site-specific, but generic or overall project tasks that are required to install hardware, software, and/or databases, prepare data, validate the solution for use,	Canada will evaluate the degree to which the Bidder's proposed approach to implementation: (a) will be effective in meeting the requirements of this Solicitation; (b) demonstrates best value to Canada; (c) is flexible and demonstrates capability to adapt to change; (d) demonstrates a reduction of risk to Canada; and (e) demonstrates the full implementation of the EPS in accordance with the SOW.

		and on-boarding of users in accordance with the requirements of this Solicitation; ii. identification of critical dependencies; iii. the resources (including their job titles and roles) required to accomplish each task; iv. the criteria for successful completion of each of the major tasks; v. a high level plan for the transition to full operations*; vi. a description of your user acceptance testing process for the delivery of each deployed functionality; vii. the Work Breakdown Structure and GANTT chart; viii. the recommended priority and sequence for addressing the elements of implementation and the supporting rationale for these recommendations; ix. a proposed issues management and resolution process; and x. the Bidder's approach to managing ongoing change to the implementation plan. * For the purpose of this criteria full operations means having achieved all the Transition-in Milestones as outlined in 7.5.2.9 in the SOW and the Service Desk is operational in accordance with 4.7 in the SOW.	
R2.2	Training Plan	The Bidder should describe its approach to the development and delivery of training and explain how it will be effective in achieving the training	Canada will evaluate the degree to which the Bidder's training approach is feasible and consistent with the

		objectives and requirements of this Solicitation, including: i. a description of the approach used for initial training and regenerative training for each of the user communities; and ii. a description of the recommended priority and sequence of training, including the supporting rationale for these recommendations; and iii. how the training will be kept current with EPS as it is upgraded, processes are updated, as well as aligns with best practices for delivery of training	training objectives and requirements of this Solicitation by considering: (a) the comprehensiveness of the measures included in the proposed training approach; (b) the degree to which the response demonstrates how the approach can be applied effectively to all user communities and kept current with each major release throughout the Contract; (c) the degree to which the training will be updated to deal with user performance issues; and (d) the use of good industry practices, including interactive eLearning technologies.
R2.3	Change Management and Communication Plan	The Bidder should describe its approach to change management and communication to the various user communities; how it will be used throughout the implementation and the roll-out of the EPS; and explain how it will be effective in achieving the change management and communication requirements of this Solicitation.	Canada will evaluate the degree to which the Bidder's approach to change management demonstrates that: (a) it increases awareness to the various user classes during the implementation and roll-out of the EPS; (b) it encourages adoption by the various user classes during roll-out; and (c) it is feasible and takes into consideration GC Legislation and Policies.
R3	**Management Approach**		
R3.1	Organizational Structure and Use	The Bidder should describe the organizational model proposed to deliver all elements of this Solicitation and explain how it will be effective in meeting the requirements of this Solicitation, including:	Canada will evaluate the degree to which the bid demonstrates a cost-effective and responsive organizational model and by considering:

		i. providing an organization chart and a description of each of the positions proposed for its organization including type, level, quantity, functions performed and typical qualifications; ii. providing a breakdown of the positions and functions whose costs would be included in the on-going solution fees or as part of the implementation costs; iii. indicating which services will be delivered through the use of internal resources and which will be delivered through subcontractors, joint-venture members or other business partners; iv. describing why the proposed delivery method represents best value for Canada; v. describing the proposed organizational strategy for assigning functions to and managing relationships between Bidder's internal resources, subcontractors, joint-venture members, and business partners and how this strategy will provide best value to Canada; vi. describing the Bidder's approach to ensuring appropriate skills are developed and maintained for resources rendering services under the SOW; vii. indicating how the proposed organization will address the requirements of this Solicitation; and	(a) the degree to which the organizational structure and strategy will be effective in meeting the requirements of this Solicitation; (b) the degree to which the organizational model demonstrates best value to Canada; (c) the flexibility of the organizational model to adapt to change, including changes in the volume of work; and (d) the effectiveness of the governance model.

		viii. describing the governance model associated with the proposed structure and how this ensures clear lines of accountability, integration between the different functional areas involved in delivering services, effective management of risk, and responsiveness to issues and requests that may come up during the contract.	
R3.2	Risk Management	The Bidder should describe its approach to risk management. The approach should address risks that may impact the successful delivery of the EPS, considering all expectations as described in this Solicitation. The Bidder should rely on and use its past experience on projects of similar nature and scope as the services described in this Solicitation to identify these potential risks. Each risk should be clearly described and should contain enough information to describe to Canada why the risk is a valid risk. The Bidder should explain how it will avoid the risk or minimize the chances of the risk occurring. If the Bidder has a unique method to minimize the risk, the Bidder should clearly explain it. The Bidder's approach to risk management should be broken down into two subparts: Assessment of Controllable Risks and Assessment of Non-Controllable Risks.	Canada will evaluate the degree to which the Bidder's approach to risk management demonstrates: (a) an ability to visualize, understand, and minimize or eliminate risk to Canada; (b) how it will lead to a successful implementation of the EPS; (c) risks that may cause the project to not to be completed on-time or within budget; (d) an ability to address risks that may generate change orders or be a source of dissatisfaction for Canada; and (e) how it will reduce the impact of risks on the performance of the Contract and increase the reliability of the services provided.

		A**ssessment of Controllable Risks**: This should include risks, activities, or tasks that are controllable by the Bidder, or by entities/individuals that are contracted by the Bidder. This should include things that are part of the technical scope of what the Bidder is being hired to do. This may also include risks that have already been minimized before the project begins due to the Bidder's expertise (e.g. risks that are no longer risks due to the Bidder's expertise in delivering this type of project). All risks and strategies to mitigate these controllable risks should be included in the Bidder's financial proposal. **Assessment of Non-Controllable Risks**: This should include risks, activities, or tasks that are not controllable by the Bidder. This may include risks that are controlled by Canada, risks that are caused by outside agencies, or completely uncontrollable risks. Although these risks may not be controlled by the Bidder, the Bidder should identify a strategy that can be followed or used to mitigate these risks.	
R3.3	Relationship Management	The desired relationship between the Bidder and Canada includes a strong degree of interaction, open two-way communication, and helping the GC achieve its objectives. The Bidder should provide its proposed strategy for building an effective and positive working	Canada will evaluate the degree to which the Bidder's proposed strategy for the working relationship between the Bidder and Canada demonstrates: (a) that it is effective at building a successful and positive working relationship between the Bidder's team and Canada;

		relationship between the Bidder's team and Canada. The description should include: i. clear channels for communicating issues, agreeing on resolutions and for updates on new services and technologies; ii. the name and brief profile of the most senior executive directly responsible for this Contract including its proposed role and responsibilities; and iii. the proposed approach to the relationship between the Bidder's senior executive responsible for this Contract and the Project Authority, including the frequency with which they will meet to review performance and other issues.	(b) that Canada has the authority for managing configuration to the EPS; (c)the Bidder's responsibility to Canada and to its own team to provide effective corporate support in the areas of implementation, training, support, maintenance and service quality; (d) the consistency and effectiveness of communication between all parties is ensured; (e) the interaction and integration among team members in different functional activities is encouraged to develop innovative ideas and resolve problems; (f) the processes and methods of dealing with conflict resolution procedures and problem-solving mechanisms; and (g) The feasibility of the Bidder's process for the Project Authority to be able to contact the Bidder's senior executive responsible for the contract during hours of operation and all off-hours including weekends and holidays.
R3.4	Service Desk Support	While the program is focused on e-enabled service delivery, the Contractor must provide a secure service desk, accessible by all user communities, to provide support in the use of EPS and to resolve users' technical challenges. The Bidder should describe its approach to service desk services to meet the requirements of this	Canada will evaluate the degree to which the Bidder's approach to service desk services: (a) makes effective use of procedures derived from the ITIL or ISO processes for Service Request and Incident Management; (b) has an effective service desk performance reporting mechanism;

		Solicitation, particularly the Service Desk section of the SOW, including how it will: v. manage the scalability and de-scalability of the services as the solution responds to the demand for use; vi. categorize, prioritize and log all incidents (e.g. inquiries, issues, service requests) vii. document, manage and track all incidents, service requests and inquiries, regardless of the means by which they are submitted (e.g. by telephone, e-mail, fax or direct online input by users) viii. identify, forward, escalate (e.g. Level 2 and Level 3 escalation), manage incident resolution and close incidents and service requests – including those escalated to third parties; ix. identify and describe priorities, response and resolution targets for incidents and service requests that have different impacts; and iv. log, track, manage and report on service desk utilization.	(c) ensures adherence to service levels and performance metrics; and (d) manages scalability and de-scalability of the service desk services.
R3.5	Innovation and Value Added	The Bidder should provide innovative ideas and identify any value added offerings that may benefit Canada. If the Bidder can include more scope or service within the constraints of Canada, the Bidder should provide an outline of the potential value added.	Canada will evaluate the degree to which the Bidder demonstrates: (a) additional EPS functionality not included in this Solicitation that are of value to Canada; (b) additional services that are not included in this Solicitation that are of value to Canada;

		The items proposed will be incorporated in the Contract, if they are accepted by Canada. The cost must be included as part of the Bidder's Financial Bid.	(c) a significant improvement to the timelines identified in this Solicitation (d) best value to Canada; and (e) how the innovative ideas or value added offerings: o will be effective in meeting the requirements of the Solicitation; o are feasible and take into consideration GC Legislation and Policies; and o will contribute to the overall quality of operations. Any services bid against this criteria must be in compliance with the terms and conditions of the resultant Contract. Should they not be in compliance, they will not be considered by Canada in the evaluation. The price for any services bid against this criteria must be included as part of the basis of payment as requested in this RFP– no new basis of payment will be considered. Should the services not comply with the stated basis of payment, they will not be considered by Canada in this evaluation. Failure to do so will result in Canada not considering the related items proposed by the Bidder in the Technical Evaluation.
R3.6	Product Roadmap	The Bidder should describe its product roadmap strategy for ongoing development of EPS services, including:	Canada will evaluate the degree to which: (a) the strategy is effectively managed and communicated to the clients;

		i. what influences the product roadmap (e.g. competition, market positioning, customer requirements, etc.); ii. the Bidder's communication plan to its clients; iii. how are clients' requirements incorporated into the strategy (e.g. client advisory council); and iv. the key functionality and services that are a part of the Bidder's Product Road Map.	(b) Canada will have the ability to influence the product roadmap(s); and (c) current and ongoing development of EPS services are envisioned in the Bidder's long term plans.
R4	**IT Technical Criteria**		
R4.1	Technical Deployment Model – SaaS	The Bidder should describe the overall approach for the technical deployment model to be used for the EPS, including: i. a description of the proposed model for the EPS and the approach for deployment through different project waves, including but not limited to: o management of data and processes in the Bidder's EPS; o description of supporting technology stack; o infrastructure management plan; o system configuration, customization; and o integration and interoperability plan as the EPS is rolled out.	Canada will evaluate that the Bidder's cloud deployment model demonstrates throughout the different project waves: (a) A high degree of reliability; (b) A high degree of the scalability of EPS; and (c) Robust performance of EPS.

		ii. a description of how the deployed model can meet the scalability and performance Service Level Agreements (SLAs) described in this Solicitation including through peak periods in business cycles; and iii. a data management plan for the EPS and, if required, a master data plan for Canada.	
R4.2	Technical Architecture	The Bidder should provide multiple Technical Architecture diagrams, both conceptual and logical, for the different architectural views of the EPS, labelled as follows: i. application ii. technology iii. integration iv. business	Canada will evaluate the degree to which: (a) the different architecture views of the overall solution architecture interact with each other; (b) the model uses n-tier architecture; (c) service-oriented architecture (SOA) is employed; and (d) the business and application architecture aligns with the requirements of this Solicitation.
R4.3	Technical Integration	The Bidder should describe its approach to the integration of the EPS with Canada's other systems, including: i. its proposed interoperability methods and technology to integrate with Canada's systems;	Canada will evaluate the degree to which the Bidder demonstrates that the EPS is equipped with technology and tools required for integrating its services to Canada's support and back-office systems and understands the interoperability needs by describing the degree to which: (a) the integration architecture and tools supports Canada's system interfaces requirements in this Solicitation;

		ii. a listing of pre-built Application Program Interfaces (APIs) and Web Services that will be used to push and pull data. The Bidder should indicate which open standards will be used and whether they will be secured and/or encrypted; iii. a description of how the EPS will interoperate with multiple Departmental Financial Materiel Management Systems (DFMS) (e.g. SAP) which may use distinct business processes and unique chart of accounts; and iv. a Master Data Management approach as it pertains to interoperability and integration.	(b) the scale of the proposed EPS's existing API libraries supports the interoperability with leading ERP products; and (c) Web Services and APIs make use of open-standards.
R4.4	IT Service Continuity Plan	The Bidder should describe its approach to ensuring continuity of EPS services, including: i. its approach to service continuity that includes its incident management process and help desk support and any exceptions to continuity; ii. its approach to disaster recovery that includes an exercise schedule, roles and responsibilities and communication protocol; and	Canada will evaluate the degree to which the Bidder demonstrates that the EPS is designed and operates in a manner that will provide continued IT services, meeting and/or exceeding the SLAs described in this Solicitation by describing the degree to which: (a) the Bidder's back-up plans support IT service continuity; (b) the Bidder's approach to disaster recovery and service continuity supports the restoration of the system; and (c) the Bidder is able to export all of Canada's data in escrow, in a format readable by Canada as described in this Solicitation, and have the capability to transfer to another service provider.

		iii. its approach to data escrow.	
R5	**Security Plan**		
R5.1	IT Security Policies and Procedures (Controls)	The Contractor will be required during the Term of the Contract to have and maintain policies and procedures that support IT Security and will address the technical, operational and maintenance security areas. The Bidder should demonstrate its ability to comply with these requirements by providing evidence of any existing policies that support the security control families described in Annex 2 and ITSG-33. The Bidder should describe how its policies and procedures align to the security control families by providing the following information on current policies and procedures: (a) name of policy and/or procedure (b) its purpose (c) its scope (d) the roles and responsibilities that are described within the policy and/or procedure (e) how it ensures coordination among organizational entities	Canada will evaluate the degree to which the Bidder's response demonstrates thoroughness, effectiveness and meet or exceed the security control families described in Annex 2 of this Solicitation and ITSG-33.

		(f) how it ensures compliance within the organization Note: Canada reserves the right to request all the reference material as indicated in the Bidder's response.	
R5.2	IT Security Topology Diagram	The Bidder should provide an IT security topology diagram which should include the following components: i. interfaces ii. web iii. applications iv. databases v. security devices vi. system management vii. backup infrastructure	Canada will evaluate the degree to which the Bidder's IT security topology diagram demonstrates that the overall design provides a secure environment.
R5.3	Forensic Procedures and Safeguards	The Bidder should provide its proposed approach to forensic procedures and safeguards.	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to forensic procedures and safeguards: (a) will support forensic investigations and provide safeguards for assets; and (b) will ensure the collection, retention, and preservation of forensic and audit evidence.
R5.4	Security Organization	The Bidder should describe the experience of the security organization that will be responsible in ensuring the security of EPS, including the name of	Canada will evaluate the degree to which the Bidder's security organization demonstrates:

		each person, their role & description of their duties, their experience, and certifications.	(a) The experience of the personnel supporting EPS; (b) The relevancy of the certifications of the personnel; (c) The roles and the description of the duties of the personnel (d) How the personnel stay current with security trends.
R5.5	Data Segregation	The Bidder should provide its proposed approach to data segregation, that should include: i. information system design documentation; ii. information system architecture; and iii. information system configuration setting and associated documentation.	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to data segregation: (a) provides logical data segregation management; and (b) provides a breadth of data segregation for Canada's data throughout all aspects of the system's functionalities and system administration.
R5.6	Disposal	The Bidder should provide its proposed approach to the disposal of Canada's data, including: i. a plan for hard-drive sanitation or an action plan if the system is hosted in a virtual environment that will ensure Canada's data is not obtainable; ii. a plan for data disposal; iii. system disposal processes and procedures;	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to the disposal of Canada's data: (a) meets the requirements for disposal of data and IT assets as outlined in Annex 2 of this Solicitation; and (b) aligns with Annex 2 of ITSG-33.

		iv. a plan for destruction of duplicate records that may be stored in a records management system; and v. the process it plans to follow when the system is no longer required and is being decommissioned.	
R5.7	Continuous Monitoring Service	The Bidder should provide its proposed approach to continuous monitoring of EPS and include the following components: i. The strategy for continuous monitoring based on defined risk tolerance. ii. Established measures, metrics, and status monitoring and control assessments frequencies. iii. Details of data collection for the defined measures and its reporting aspects. iv. Analysis methods of the data gathered and Report findings accompanied by recommendations. v. Response mechanisms to assessment findings to include making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority.	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to continuous monitoring of EPS provides: (a) High operational visibility; (b) strong, effective, and efficient change control management; and (c) adherence to incident response duties as outlined in the Solicitation.

		vi. Review and Update cycles to support continuous improvement and maturing measurement capabilities.	
R5.8	Industry IT Security Certification	The Bidder should provide proof of its security certification(s) in the form of a copy of a valid certificate and describe how the certification was assessed and obtained (e.g.: 3rd party, self-assessment) for each IT Security certification held, such as: i. FedRamp; ii. Cloud Security Alliance – STAR; iii. COBIT; iv. ISO 27001; and v. others.	Canada will evaluate the degree to which the Bidder demonstrates: (a) the relevancy of the role of the member of the Bidder's team (e.g. Joint-Venture member, subcontractor) who holds the certification; (b) rigor in how the certifications were obtained; and (c) the relevancy of the Bidder's certifications to the requirements of this Solicitation.
R5.9	Identity, Credential and Access Management	The Bidder should provide details on its proposed solution's Identity, Credential and Access Management level of assurance capabilities with respect to CSE guidance ITSG-31A. The Bidder should identify the level of assurance and demonstrate how it meets the requirements of that level.	Canada will evaluate based on the following: a) No Level = 0 points b) Level 1 = 0.5 points c) Level 2 = 1.75 points d) Level 3 = 2.25 points Maximum 2.25 points.

R6	Additional Functional Requirements	
R6.1	Additional Functional Requirements - GENERAL	
R6.1.1	In addition to the functionality identified in Part 5, A-10 Workflow - General of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to support built-in tutorials to facilitate the configuration of a workflow by authorized administrators.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
R6.1.2	In addition to the functionality identified in Part 5, A-11 Workload – Tracking and Status of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for authorized administrators to configure display formats, business rules and set indicators and alarm triggers for tracking the status of individual and team workloads (e.g. based on the commodity).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.54 points
	II. to display individual and team procurement workload information in various formats including, but not limited to, tabular, graphs, charts.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	III. to display workload indicators and trigger alarms based on the procurement file activities and individual or group workloads.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.54 points
	IV. for users to sort, filter and aggregate workload items.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.54 points
	V. for authorized administrators to track procurement pipeline and provide insight into planned procurement activities and when they need to be executed.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
R6.2	Additional Functional Requirements – SOURCING AND CONTRACT MANAGEMENT	
R6.2.1	In addition to the functionality identified in Part 5, C- 01 Sourcing and Contract Management - Requisition Management of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for the Contracting Officer to group and consolidate similar requirements based on a variety of parameters such as,	The Bidder cannot provide this functionality = 0 points

	but not limited to, commodity type, method of procurement, Delivery location, from different requisitions to facilitate group buying.	The Bidder will provide this functionality = 0.78 points
R6.2.2	In addition to the functionality identified in Part 5, C- 02 Sourcing and Contract Management - Planning and Strategy Development of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for the authorized administrators to create and configure and manage a variety of procurement templates that will assist Contracting Officer during planning and strategy development phase.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	II. for the authorized administrators to configure and manage access to various information sources that are external and internal to the solution including, but not limited to, relevant policies, rules and regulations (e.g. hyperlink to a policy that resides outside or inside of the solution).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	III. for the Contracting Officer to access various internal and external information sources at any time during planning and strategy development.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
R6.2.3	In addition to the functionality identified in Part 5, C- 03 Sourcing and Contract Management - RFx Creation of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for the authorized administrators to configure triggers and alerts for other user's activities that have to be performed based on pre-established set of rules.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	II. for multiple users to simultaneously work on and complete different sections of an RFx.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	III. for the Contracting Officer to preview layout and design of all configured forms(e.g. solicitation, evaluation matrix, pricing tables etc...).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
R6.2.4	In addition to the functionality identified in Part 5, C- 04 Sourcing and Contract Management - RFx Publishing of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	

	I. for the Contracting Officer to configure a bidding clock in real time which supports time zones and automatically adjust for daylight savings time.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	II. to display an event countdown clock to show the time remaining for sourcing event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	III. for authorized administrators to control whether bid opening is permitted during bidding period (e.g. before closing date for on-going opportunities).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
R6.2.5	In addition to the functionality identified in Part 5, C- 05 Sourcing and Contract Management - Bid Submission of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to guide supplier through the bid submission process (e.g. checklist or wizard).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.26 points
	II. to manage a multi-envelope electronic bidding process by allowing supplier to organize and submit their bids in multiple sealed envelopes (e.g. one technical, one financial and one certification).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	III. to display a summary of supplier bid for a final review prior to submission.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	IV. to link bid attachments with related RFx sections and/or individual RFx requirements.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	V. to enable supplier to import, edit and carry forward answers from previous sourcing events for the purpose of responding to repetitive requirements (e.g. ask once – tell once).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	VI. for the supplier to provide reference information about posted bonds, security deposits or cheques with their bid submission.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points

	VII. to automatically check and validate completeness of the suppliers' responses.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
R6.2.6	In addition to the functionality identified in Part 5, C- 06 Sourcing and Contract Management - Bid Evaluation of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to support a secure virtual evaluation environment through defined parameters and permissions set by authorized administrators through administration properties.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	II. for the Contracting Officer to set on/off permissions for collaboration between participants during the evaluation process.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	III. to compare and assess responses and capabilities of one or multiple suppliers against predefined questions.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	IV. to perform comparative evaluation of bids at the same time including, but not limited to, evaluation: a. on each item from a basket of goods b. group of items c. a whole basket of goods	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	V. for the Contracting Officer to configure the technical and financial evaluation to only evaluate certain items in the catalogue file in order to conduct a 'basket of goods' financial evaluation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	VI. for the Contracting Officer to select and approve individual line items that a supplier is qualified for as a result of a technical and financial bid evaluation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	VII. for evaluators to perform scenario analysis during bid evaluation (e.g. generate multiple optimization scenarios per sourcing event).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.26 points

	VIII. to support Bid Optimization scenario analysis by using various parameters and constraints including, but not limited to: a. non-financial criteria; b. matrices and tiers; and c. responses to RFx questions.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	IX. for the Contracting Officer to generate an overall bid evaluation summary that includes: a. each stage of the bidding process; b. individual and overall suppliers scores; c. consensus results with comments by evaluators; d. qualitative and quantitative ranking; e. overall cycle time; and f. tabulated results of the ratings (as applicable to the RFx).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	X. for the Contracting Officer to select and identify proposed winner(s) and notify all stakeholders of the result.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
R6.2.7	In addition to the functionality identified in Part 5, C- 07 Sourcing and Contract Management - Contract Award of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for the Contracting Officer to configure and send notices to bidders to advise them about outcome of the solicitation process (e.g. Letters of Regret).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	II. to link the results of evaluation process to relevant contract award templates such as, but not limited to Letter of Regret, Contract Award Notice.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	III. to create the list of users who will be receiving a notification of the contract award.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.26 points
R6.2.8	In addition to the functionality identified in Part 5, C- 08 Sourcing and Contract Management - Contract Administration of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	

	I. to establish contract management milestones and bring forwards (BFs) at various stages of the contract (e.g. configuring auto notifications for contract milestones, transition periods, contract extensions).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
R6.2.9	In addition to the functionality identified in Part 5, C- 10 Sourcing and Contract Management - Central Repository of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to link both versions (English and French) of the clause so that when a clause is referenced in the English version it is automatically referenced and/or updated in the French version or vise versa.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.78 points
	II. to make all versions of clauses and general conditions available publicly through the portal.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.52 points
	III. to store cost formulas in repository as part of templates.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.26 points
R6.3	Additional Functional Requirements – PROCUREMENT MANAGEMENT	
R6.3.1	In addition to the functionality identified in Part 5, D - 05 Catalogue - Catalogue File of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for authorized administrators to create an identifier link to indicate items that are equivalent (same fit, form, and function) to each other.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	II. to group items into optional bundles where select items can be removed by the user (e.g. extended warranty on a product).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	III. to include multiple pictures (e.g. different views) per Catalogue line item.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.55 points
	IV. to include a 360 degree model for a Catalogue item.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.28 points

R6.3.2	In addition to the functionality identified in Part 5, D - 06 Catalogue - Pricing of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for authorized administrators to configure and manage cumulative tiered price ranges that are applied to an individual order for items in a Catalogue File (e.g. tiered price would become available to a user based on cumulative orders).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	II. for authorized administrators to configure and manage bulk tiered price ranges that apply a discount to an individual order for a Catalogue File (e.g. the entire order is discounted based on a dollar amount).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	III. to connect to the applicable Consumer Price Index (CPI) table from Statistics Canada to determine the price update calculation when required by a given contract / framework agreement.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
R6.3.3	In addition to the functionality identified in Part 5, D - 08 Catalogue - Shopping Cart - General of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to calculate the distance (air, or ground using existing infrastructure, not "as the crow flies") between multiple points to determine the overall cost (e.g. number of KMs times cost per KM).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	II. to provide a configurable print layout of the Shopping Cart request.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.28 points
R6.3.4	In addition to the functionality identified in Part 5, D - 09 Catalogue - Shopping Cart - Search of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for a cross-PunchOut search for an item.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	II. to suggest complementary or related products/services (cross-selling) that are brand agnostic for the user's	The Bidder cannot provide this functionality = 0 points

	selected goods or service (e.g. laptop would suggest a bag, warranty, installation service).	The Bidder will provide this functionality = 0.28 points
R6.3.5	In addition to the functionality identified in Part 5, D - 10 Catalogue - Shopping Cart - Creation of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to provide intelligent defaulting of financial codes based on user, department, supplier, commodity, item, or any combination thereof on the Shopping Cart request line item.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.55 points
	II. to identify a Shopping Cart request as either a capital asset or an operating expense based on at least one of the following methods: - user selection - GL Account - Commodity Code	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.28 points
	III. to have the supplier select an authorized dealer, reseller, or agent of a good or service (e.g. vehicles) nearest the postal code of the delivery location if one is not specified by the client.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
R6.3.6	In addition to the functionality identified in Part 5, D - 11 Catalogue - Shopping Cart - Display of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to display products recently viewed by the user.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.28 points
	II. to display a single page summary screen of the Shopping Cart request for workflow approval and prior to submitting it to a Supplier.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.55 points
R6.3.7	In addition to the functionality identified in Part 5, D - 12 Catalogue - Shopping Cart - Inventory of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for suppliers to update goods or service availability status configured to update on a real time, scheduled batch, or manual basis.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points

R6.3.8	In addition to the functionality identified in Part 5, D - 13 Catalogue - Shopping Cart - Management of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for users to copy an existing Order and create an editable Shopping Cart request accessible by a select set of users.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.81 points
	II. for users to create a Shopping Cart request with a standard order to be made at scheduled intervals (e.g. monthly paper order).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.55 points
R6.4	Additional Functional Requirements – SERVICE PROCUREMENT	
R6.4.1	In addition to the functionality identified in Part 5, E - 02 Service Procurement - Catalogue - Management Creation of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to authorized administrators to configure authorized access to view and change resource qualifications for specific resource categories or sub-categories.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	II. for suppliers to indicate if they have a local office in the applicable region within the Catalogue and for authorized administrators to configure when this information is displayed to a user in the ordering process.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.8 points
	III. for suppliers to indicate at which locations they offer specific services (e.g. what aircraft are available at an air base) within the Catalogue to assist the user in the selection of a supplier during the ordering process.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
R6.4.2	In addition to the functionality identified in Part 5, E - 03 Service Procurement - Shopping Cart - General of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for suppliers to submit questions in relation to a Shopping Cart request and for the user to meta tag the question and to publish and edit the question and response in both official languages during the response period for all suppliers to view (e.g. Q/A form) without the supplier name being published.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points

	II. for authorized administrators to view the status of the supplier's response to a specific Order (e.g. indicated no interest, evaluated but rejected, not yet invited, Order issued) within invited supplier list during the ordering process.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	III. to authorized administrators to configure the evaluation status of proposed resources (e.g. viewed, under evaluation, shortlisted, accepted, rejected) and to display and configure certain notifications to be sent to suppliers regarding the respective status.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.8 points
R6.4.3	In addition to the functionality identified in Part 5, E - 04 Service Procurement - Shopping Cart - Creation of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to inform the user of invited suppliers' preference of language for each respective Method of Supply and regional level prior to creating the Shopping Cart request.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	II. to apply milestone payments based on a configured amount of the total Order value stated in the Shopping Cart request (e.g. Supplier receives $40,000 for delivering Milestone 1, and remaining $60,000 for Milestone 2).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
R6.4.4	In addition to the functionality identified in Part 5, E - 06 Service Procurement - SOW Management - General of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to source multiple resources under one SOW with a single supplier (e.g. both Business Analyst and Project Manager from Company A).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	II. to split a SOW for multiple resources into a multi-awarded supplier contract (e.g. Business Analyst from Company A and Project Manager from Company B).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	III. for users to configure the applicable payment percentage that is to be attached to each milestone in the Shopping Cart request (e.g. Supplier receives 40% of payment for	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points

	delivering Milestone 1, and remaining 60% for delivering Milestone 2).	
R6.4.5	In addition to the functionality identified in Part 5, E - 09 Service Procurement - SOW Management - SOW Builder of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for users to save newly created sections in the SOW builder repository.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.8 points
R6.4.6	In addition to the functionality identified in Part 5, E - 11 Service Procurement - SOW Management - SOW Amendments of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to redline amendments made to a SOW which will automatically be tracked in a change log, including the dates the changes were made and by which user.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	II. for users to select which version of the SOW they want to compare the redlined amendments to (e.g. want to only view the redlines between versions 3 and 4 of the SOW, hiding all amendments made before this time).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	III. to send SOW amendments to proceed through an approval workflow prior to being published.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	IV. to present an updated version of the SOW without the redline changes.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
R6.4.7	In addition to the functionality identified in Part 5, E - 13 Service Procurement - Resource Management - Performance Management of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for users to configure scheduled individual resource performance reviews for the client to complete on a periodic basis (e.g. every 2 months, at end of contract only).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
R6.4.8	In addition to the functionality identified in Part 5, E - 14 Service Procurement - Master Resource Record of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	

	I.	for authorized administrators to activate and deactivate resource profiles.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	II.	for suppliers to maintain their version of the proposal resource profile for a specific resource (e.g. if there is more than one supplier proposing the same resource) and update the qualifications, with the option for the user to view both the redline changes and final versions.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	III.	for authorized administrators to conduct and capture a project reference check to validate the accuracy of the proposed resources qualifications and experience related to that reference presented by the supplier.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	IV.	to identify if an individual resource or supplier has previously done work for the client organization.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.8 points
	V.	for individual organizations to create and manage configurable onboarding and offboarding activities for individual resources for a specific contract (e.g. assigning assets/inventory, issuing security IDs), with the ability to attach accompanying documentation and assign an owner to each activity.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
	VI.	to track the status of onboarding and offboarding activities and to configure dates of which to escalate non-completed activities by sending a notification to the appropriate user (e.g. the non-disclosure agreement for a specific resource has not been signed yet, marking it as incomplete).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.2 points
R6.5	Additional Functional Requirements – BUSINESS INTELLIGENCE		
R6.5.1	In addition to the functionality identified in Part 5, G - 01 Business Intelligence - General of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:		

	I. for authorized administrators to create, manage and publish standard report templates and make them available to other users.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.24 points
	II. for users to manage, organize and store an unlimited number of reports for various reports types and categories.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
R6.5.2	In addition to the functionality identified in Part 5, G - 02 Business Intelligence - Reporting of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for users to generate drill-through reports to view information at a specific level, and drill to other levels of information on a user-selected value.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	II. for users to generate static "point in time" reports and save them for future use.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	III. to enable users to build their own custom queries and reports using the solution's ad-hoc query and reporting tool that has a reusable semantic layer with familiar and common business terms that allows user, without being technically savvy, to: a. navigate available data sources; b. access predefined metrics; c. navigate hierarchies.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	IV. to generate report on the status and data matrices of procurement opportunities such as, but not limited to: a. number of procurement opportunities and their status; b. processing time (e.g. by Supplier, By Client etc..); c. number of transactions (e.g. user actions, number of purchases etc.); and d. approval stage and status.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	V. to generate reports that can rank suppliers and show trends in supplier performance over time based on various	The Bidder cannot provide this functionality = 0 points

		collected data, such as, but not limited to: a. quality; b. supplier's delivery performance; and c. service performance.	The Bidder will provide this functionality = 0.24 points
	VI.	to generate spend reports that can show various summary and detail reports such as, but not limited to: a. potential savings; b. year over year Spend by commodity categories and supplier; c. cumulative Spend by purchase order and by invoices; and d. Spend reports for supply arrangements and standing offers by various parameters (e.g. by supplier, region, etc.).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	VII.	to generate reports on user and group access to individual solution components and objects, including but not restricted to: a. full and partial access to procurement file(s); b. user and group functionality rights, privileges and restrictions for assigned components; c. user and group information access rights, privileges and restrictions; and d. user and group access to meta-data properties.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.12 points
R6.5.3	In addition to the functionality identified in Part 5, G - 03 Business Intelligence - Analytics of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:		
	I.	to support line item level Business Intelligence and detailed analysis (i.e. how many units of an item were purchased, by who, from whom, for how much, and under what contract).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	II.	to analyse and calculate the growth of processed transactions within a specific time period by various parameters (e.g. by supplier, by client).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.24 points

R6.5.4	In addition to the functionality identified in Part 5, G - 04 Business Intelligence - Reporting and Analytic Dashboard of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to enable and support a broad range of Business Intelligence data visualization tools including, but not limited to: a. display of multiple diverse objects on a page like table, picture and text; b. various types of Charts (e.g. Bar, scatter, combination, pivot, line, radar, area, high-low, stacked bar); c. various types of graphs with target indicators (e.g. Line, bullet, bubble) d. meters and gauges; and e. 2D and 3D charts and graphs.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	II. for users to Configure and create highly interactive reporting and analytic dashboards and define metrics and data content with visual exploration and embedded advanced analytics.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	III. for users to configure and create reporting and analytical dashboards with operational and strategic information that allow things such as, but not limited to: a. production, distribution and printing of reports and widgets b. configuration of parameters, filters and prompts c. guided dashboard navigation	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	IV. for users to configure and generate a dashboard report that shows all sourcing initiatives in progress, their status and timelines.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
	V. for users to configure and generate custom data views on reporting and analytic dashboards and reporting pages.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.24 points

	VI. for users to seamlessly move from reporting and analytic dashboard to all relevant procurement modules and spend management applications.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points
R6.6	Additional Functional Requirements – SUPPLIER RELATIONSHIP MANAGEMENT	
R6.6.1	In addition to the functionality identified in Part 5, H - 01 Supplier Relationship Management - Supplier Profile Management of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. for authorized administrators to configure business rules and set parameters for supplier's activation/deactivation including but not limited to: a. authorized user turns on/off functionality to activate/deactivate supplier; and b. system automatically activates/deactivates supplier's accounts parameters.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	II. to pre-populate supplier registration form with information and data from other systems and enable a supplier to maintain their own information including, but not limited to: a. name, address, contact information; b. aboriginal owned; c. controlled goods registration; d. financial Statements; e. direct deposit payment information; f. Ghost Card credit information; and g. special characteristics of their business.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
R6.6.2	In addition to the functionality identified in Part 5, H - 02 Supplier Relationship Management - Performance of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to maintain a repository of surveys and scorecards which is accessible only through Role Based Access and organized in a number of ways, including, but not limited to: a. contracts;	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points

		b. framework agreements; and c. suppliers.	
	II.	for authorized administrators to configure and create separate survey versions specific to a particular subject including, but not limited to: a. geographic location; b. procurement; and c. stakeholder.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	III.	for authorized administrators to configure and schedule survey.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
	IV.	for users to define, update and maintain Key Performance Indicators as part of performance management process.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	V.	to define maximum and target points for each Key Performance Indicator for a supplier or category.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	VI.	to raise a flag and notify a configurable list of users when Key Performance Indicator score is below established targets.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
	VII.	to map survey questions to specific Key Performance Indicators and automatically pull in data from survey responses to pre-populate a scorecard.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
	VIII.	to consolidate and merge results from multiple surveys into a single scorecard.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	IX.	to route scorecards for review by identified users.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	X.	for users to collaborate with suppliers on scorecard results and associated action items.	The Bidder cannot provide this functionality = 0 points

			The Bidder will provide this functionality = 0.72 points
	XI.	for suppliers to have 'view-only' access to their scorecards and survey results.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	XII.	to pull in qualitative and quantitative data from both third party sources and from within the solution as part of scorecard generation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
	XIII.	to support various scorecard features, including, but not limited to: a. graphing of scorecard results; b. generating scorecards for different level of performance (e.g. performance is above, at-risk or below targets); and c. rank suppliers for specific commodities by weighing scores on score carding (e.g. highest and lowest).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
R6.6.3	In addition to the functionality identified in Part 5, H - 03 Supplier Relationship Management – Evaluation Tools of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:		
	I.	for authorized administrators to copy previously created surveys for re-use.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points
	II.	to allow survey creator/respondents to save partially built/completed surveys as drafts to be completed at some future point in time.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	III.	to allow survey creator to identify and select target survey respondents based on various parameters, including, but not limited to: a. their geographic location; and b. commodity.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	IV.	to allow survey creator and respondents to add attachments to survey with no limit on the number or size of the attachments.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.72 points

	V. to distribute and track who responds to surveys with time and date stamp of response.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	VI. to integrate survey distribution and approval with workflow including but not limited to: a. route the survey to respondents and approvers; and b. approve posting of survey results to a scorecard.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
R6.6.4	In addition to the functionality identified in Part 5, H - 05 Supplier Relationship Management - Notification of the SOW, the bidder should indicate which of the following functionality it will provide for these requirements:	
	I. to allow configuration by authorized administrators of various notification features for all activities in Supplier Relationship Management module such as, but not limited to: a. reminders that can be sent to survey participants; b. email messages as part of survey; c. scheduling of automatic events, triggers and alerts; and d. allow users to turn on/off automatic notification functionality.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	II. to track and automatically notify Contracting Officer and Supplier about need for regular update and renewal of supplier's profile information including but not limited to: a. qualifications and certifications renewal due; b. security clearance information; and c. Supplier's status (active or inactive based on a set of configurable rules).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 1.08 points
	III. for users to schedule activities and tasks associated with a supplier and notify users when tasks are scheduled to occur (e.g. a performance meeting).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 0.36 points

4. Technical Evaluation Scales

Scale 1 – Demonstrated Experience

0	**Not Addressed** – No response provided or the response does not address this Solicitation requirement.
1	**Minimally Addressed** – The proposal fails to demonstrate the experience requested due to significant deficiencies. The deficiencies or weaknesses demonstrate that the Bidder did not meet the objectives. The Bidder demonstrates limited experience and the experience is of little relevance to the solicitation requirements.
2	**Partially Addressed** – The proposal does not demonstrate that the Bidder met all of the objectives due to a significant level of deficiencies or weaknesses. However, the Bidder has some capability and demonstrates experience of some relevance the solicitation requirements.
3	**Satisfactorily Addressed** – The proposal does not demonstrate that the Bidder met all of the objectives due to a moderate level of deficiencies or weaknesses. However, the Bidder has an acceptable level of capability and demonstrates experience of adequate relevance to the solicitation requirements.
4	**Very Well Addressed** – The proposal demonstrates that the Bidder met most of the objectives with few deficiencies or weaknesses. The Bidder has a very good level of capability and demonstrates experience that is very relevant to the solicitation requirements.
5	**Excellently Addressed** – The proposal demonstrates that the Bidder met all of the objectives with very few or no deficiencies or weaknesses. The Bidder has an excellent level of capability and demonstrates experience that is highly relevant to the solicitation requirements.

Scale 2 – Generic Scale

0	**Not Addressed -** Bidder's information submitted was not relevant to the criterion or failed to submit response.
1	**Minimally Addressed** – The proposal demonstrates little understanding of the solicitation requirements and the proposed approach does not address important factors. Proposed approach has significant weaknesses and is not likely to meet solicitation requirements and does not demonstrate technical value to Canada. Proposal poses a perceived a large residual* risk to Canada.
2	**Partially Addressed** – The proposal demonstrates some understanding of the solicitation requirements and the proposed approach addresses some important factors. Proposed approach has weaknesses and is not likely to meet solicitation requirements or be effective and does not demonstrate good technical value to Canada. Proposal poses a perceived medium residual risk to Canada.
3	**Satisfactorily Addressed** – The proposal demonstrates adequate understanding of the solicitation requirements and the proposed approach addresses most factors. Proposed approach has minor weaknesses and is likely to meet solicitation requirements and provides good technical value to Canada. Proposal poses a perceived medium-low residual risk to Canada.
4	**Very Well Addressed** – The proposal demonstrates a very good understanding of the solicitation requirements and the proposed approach addresses all important factors. Proposed approach has no significant weaknesses, is likely to meet solicitation requirements, and is likely to be effective, yield very good results and provides very good technical value to Canada. Proposal poses a perceived low residual risk to Canada.
5	**Excellently Addressed** – The proposal demonstrates an excellent understanding of the solicitation requirements and the proposed approach addresses all important factors. Proposed approach has no apparent weaknesses, is likely to meet solicitation requirements, and is likely to be effective, yield excellent results and provides excellent technical value to Canada. Proposal poses very little or no apparent residual risk to Canada.

*Residual Risk is defined as the risk that remains after the Bidder's risk mitigations are considered.

5. Score Calculations

Each Criterion indicates what the Bidder should provide to support its demonstration of capability and capacity to address the Criteria as it relates to the solicitation requirements. For each Criterion, Bidders will be scored on a 0-5 rating guide using one of the applicable scale. Scores will be distributed as follows:

0 – receives 0% of the points assigned to a criterion
1 – receives 20% of the points assigned to a criterion
2 – receives 40% of the points assigned to a criterion
3 – receives 60% of the points assigned to a criterion
4 – receives 80% of the points assigned to a criterion
5 – receives 100% of the points assigned to a criterion

For example, if a proposal obtains a 3 in the evaluation of R-1.1, then the proposal's score for that criterion would be calculated as follows:

Score of 3 = 60%
Weight of criteria R.1.1 – Solution Management Services – Additional = 54 points
Therefore, 60% x 54 = 32.40 points

ATTACHMENT 3 TO PART 4:

USABILITY ASSESSMENT

Table of Contents

1. Usability Assessment Methodology: Overview

The overall objective of conducting an independent third-party review is to evaluate and benchmark the bidders' solutions from a human factors / usability perspective. Evaluating and benchmarking the performance of the solutions from a human factors and usability perspective involves focusing on the interface and interaction between the solution and its users. The evaluation will be used to observe how target users interact with each solution and the extent to which each design aligns with behaviour and expectations. Benchmarking will be used to identify the performance of each of the solutions along specific, pre-determined metrics.

The independent third-party review will consist of two lines of evidence that will be compiled into a final performance report:

a. Stage 1: Heuristic review of the solutions
b. Stage 2: Summative usability testing of the solutions with 30 participants

1.1 Stage 1: Heuristic Review

Three independent expert reviewers will evaluate each of the solutions with regards to how well it conforms against a set of usability principles – defined as heuristic criteria. These heuristic criteria will aligned with specific usability principles and will be used to measure each solution's performance from an ease of use and ease of interaction perspective.

It is imperative that the independent review conducted by each member of the expert panel be guided by a standardized assessment framework. This will eliminate any potential bias present during the review, while ensuring that the review is carried out against the lens of the solution's performance in relation to usability objectives.

(i) Proposed Heuristic Criteria:

The following table outlines the heuristic categories and individual criteria that will be used to evaluate each solution.

Heuristic Category:	Heuristic Criteria:	Weight
Help/support features	• Presence of contextual help • Discoverability • Clarity of directions	20%
Error mitigation	• Presence of in-line error prompts • Discoverability of error prompts • Clarity of the direction (is the copy clear, can the user identify the nature of the error and correct it) • Ability to correct the error and move-on • Changes / edits can be made intuitively; do not interrupt flow	15%
Navigation/flow	• Wayfinders are present to orient the user to their position in task flow / overall position within the solution	30%

	• Ability to retrace steps • Fields facilitate tabbed browsing • Language reflects user-centred language rather than institutional jargon	
Task Completion	• Clear path to initiate specific tasks (no ambiguity about starting point) • If documentation is required elsewhere – solution provides intuitive access to this (or pulls this intuitively from other data sources) • Ability to complete task within solution (no requirement to seek information outside solution to complete the task) • Input fields are clear • Input fields are formatted where applicable (e.g. date, phone number, address) rather than require manual formatting • Options for notification once task is complete (e.g. status updates) • Post-task: indications of follow-up / progress? Clarity of messaging?	35%

(ii) Heuristic Review Rating Scale:

The performance of each solution, along each heuristic criteria, will be scored using the following scale:

- 1 = Does not meet any expectations for the criteria element
- 2 = Meets a very minimum amount of the expectations for the criteria element
- 3 = Meets some of the expectations for the criteria element
- 4 = Meets most of the expectations for the criteria element
- 5 = Meets all and/or exceeds expectations for the criteria element

The three reviewers will independently score each solution against the specific heuristic metrics and document their observations. The review will be framed against the specific user tasks that will be included for the summative usability tests (see Stage 2). This will ensure that the reviewers are looking at each solution from the same context.

(iii) Heuristic Review Reporting:

The three independent reviews will then be consolidated and the scores for each heuristic element will be averaged across the three reviewers. This will create an average score for each category, as well as for each heuristic criteria. A weighted average score for each category will then be calculated.

Figure 1 provides an example of a heuristic category, specific heuristic criteria, ratings and weights. In this example, the Category: *Purpose, Scope, and Positioning Strategy* is further divided into the following criteria:

a. Home page clearly and immediately and clearly articulates purpose and scope of site
b. Site conveys firm specialization and expertise
c. Site is differentiated from competitors. Articulation of why one should visit this site instead of others
d. Articulation of why one should visit this site instead of using other channels (e.g. print materials, telephone, etc.)

This is illustrated visually in Figure 1 below (a sample evaluation matrix from a different heuristic review).

Figure 1 – Portion of a Sample Evaluation Matrix

Category	Criteria	Degree to which critiera exists (e.g. 1 = Low (does not exist); 5 = High (exists and is likely best in class; NA = not applicable or unknown)			
		Rating	Weighting factor	Weighted rating	Description
Purpose, Scope, and Positioning Strategy	Home page clearly and immediately articulates the purpose and scope of the site	4	2	8	Splash page: "...meet our exceptional people and clients, learn about our market-leading expertise, access news and insights about Canadian business law and find other valuable insights ..." Rotating Flash images indicate that this is a legal firm.
	Site conveys firm specialization and expertise	3	2	6	Home page suggests that Business Focus is cross-border legal developments, but not clear if this is focus. "Major areas of expertise" encompasses about 2 dozen areas - too diffuse.
	Site is differenatiated from competitors. Articulation of why one should visit this site instead of others	1	1	1	PDF brochure offered on home page suggesting why clients should engage firm
	Articulation of why one should visit this site instead of using other channels (e.g. print materials, telephone, etc.)	4	0.5	2	Site promotes newsletters, RSS feeds, audio podcasts - however promotion is not completely explicit.
	Average	3.00		**3.09**	

Using the heuristic categories and individual attributes as review criteria, researchers will record their findings in a scorecard as shown above in Figure 1. A 'description' column will contain annotations describing key findings of the review which can later be used to identify facilitators and barriers. The scores themselves will reflect the independent assessments of each of the researchers. Thus, each matrix, once completed and consolidated, will be considered a site scorecard or "report card", which will then facilitate comparison between the solutions.

1.2 Stage 2: Summative Usability Testing

Summative Usability Testing will be used to benchmark performance along specific usability metrics (outlined below). The usability tests will be conducted in-person with 30 participants. An interviewer will run individual usability tests with each participant, making notations of behavior, observed errors/issues and tracking performance along the specified metrics.

(i) Summative Usability Test Metrics:

The following outlines the summative usability test metrics that will be used to benchmark the performance of each solution:

a. Time to complete task (unaided)
b. Number of errors encountered
c. Ability to correct error and proceed / inability to proceed (unaided)
d. Points of abandonment
e. Number of times help sought (if contextual help available)
f. Overall success / failure rates (unaided)

The interviewer will also make notations on observations of behaviour (e.g. hesitation, confusion, delight, etc.) and will engage participants in a discussion about their experiences and impressions after each task is completed. This will help to provide a fuller annotation of participants' experiences with each solution including elements that both facilitate and act as a barrier to use.

At the end of each task, the interviewer will also administer the following four questions:

1. *How satisfied are you with your overall experience in completing this task? Please use a scale of 1 to 7, where 7 means 'Very Satisfied' and 1 means 'Very Dissatisfied'.*
2. *How satisfied are you with the ease of completing this task? Please use a scale of 1 to 7, where 7 means 'Very Satisfied' and 1 means 'Very Dissatisfied'.*
3. *How satisfied are you with the time it took to complete this task? Please use a scale of 1 to 7, where 7 means 'Very Satisfied' and 1 means 'Very Dissatisfied'.*
4. *How confident did you feel while completing this task? Please use a scale of 1 to 7, where 7 means 'Very Confident' and 1 means 'Not At All Confident'.*

In addition to the metrics outlined above, the Systems Usability Scale (SUS) will be administered at the end of the experience with each solution. The SUS is a 10 item questionnaire administered on a scale of 1 to 5, where 1 is strongly disagree and 5 is strongly agree:

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

The SUS is an industry standard questionnaire for measuring perceptions of ease of use related to particular system. It has been used to test the usability of a range of experiences, from websites to cell phones, to software, hardware and even the yellow pages. Research

has demonstrated that the SUS can be used on small sample sizes with reliable results and can effectively differentiate between usable and unusable systems. The SUS is not meant to be diagnostic – that is, to indicate where and why problems occur. As such, SUS, combined with the other usability metrics and observations of behaviour will be used to provide a full picture of the overall user experience with each solution.

(ii) Conducting the Summative Usability Tests:

One-on-one observational interviews requiring research subjects to interact with an online property to achieve relevant tasks are an excellent approach for understanding users'.

The summative usability tests will be conducted in a professional research lab in Ottawa with observational facilities (via a one-way mirror). The professional research lab has the following features;

- An interviewing room equipped with the hardware and software necessary to accommodate the full range of technological requirements necessary to conduct the test.
- An observation room sitting behind a large directional mirror, equipped with high quality speakers for transmission of session commentary, multiple monitors for streaming of on-screen activity, and comfortable work stations for up to 10 observers.
- A real-time, remote observation protocol. That is, the live transmission of on-screen activity via web-conference platform, and simultaneous transmission of session commentary via teleconference bridge, to members of the project team, at a location of their convenience.
- Post session, screen-in-screen digital recordings.

(iii) Summative Usability Test Format

As noted, each summative usability test will last 60 minutes. The interview will consist of the following components:

a. Introduction (5 minutes):
- Study purpose
- Study sponsorship
- Confidentiality of responses
- Recording
- Observers
- Moderator role and responsibilities
- Participant role and responsibilities

b. User Tasks (50 minutes):
- Use Case 1 (up to 25 minutes, including review of the experience after task completion and SUS)
- Use Case 2 (up to 25 minutes, including review of the experience after task completion and SUS)

c. Post-interaction review (5 minutes):

- Overall impressions of the solutions reviewed

(iv) Summative Usability Tasks:

To provide a framework for the usability assessment, Canada has created specific user tasks that will be conducted on each of the solutions. Each Bidder will be requested to provide a test environment for their solution that is set up for each of the user tasks identified in this Attachment.

(v) Summative Test Participant Profile

Summative usability testing is best conducted with representative members of the online property's target users. In this case, one discrete audience of interest have been identified to participate in the evaluation: Procurement Professionals

Given the number of solutions and user tasks, it will not be possible to have each participant complete each user task on every solution. Exposure to each solution and task will be rotated across the total number of interviews. This will ensure that each task and solution is evaluated an equal number of times.

Example

The following table outlines an example of the rotation order that will be followed, to allow equal exposure to the four user tasks and three solutions:

30 interviews: Assuming 20 minute scenario (user task) – 2 can be accomplished per interview (60 min interview). P1 = Participant 1, P2 = Participant 2, etc.

	Solution 1	**Solution 2**	**Solution 3**	***Total Participants Exposed to User Task:***
User Task 1	P1, P7, P13, P19, P25	P6, P12, P18, P24, P30	P4, P10, P16, P22, P28	15
User Task 2	P5, P11, P17, P23, P29	P1, P7, P13, P19, P25	P3, P9, P15, P21, P27	15
User Task 3	P3, P9, P15, P21, P27	P4, P10, P16, P22, P28	P2, P8, P14, P20, P26	15
User Task 4	P2, P8, P14, P20, P26	P5, P11, P17, P23, P29	P6, P12, P18, P24, P30	15
Total Participants Exposed to Solution:	**20**	**20**	**20**	**==**

Summary:

- User Tasks per participant: 2

- Total interview/test time per participant: 60 mins
- Max duration of user task: 20-25 mins
- Total number of participants: 30
    - Total Participants exposed to each solution: 20
    - Total participants exposed to each user task: 15

1.3 Devices for Testing

All of the interviews will be conducted in the same location and on the same device – to control for system performance and network speed. This will reduce any biases that could be introduced by conducting the summative usability tests on different devices with different performance specs. Canada will supply the device for testing *(details to be provided)* and ensure that each solution's test environment is accessible via the device.

Similarly, for the heuristic review, Canada will provide the third-party reviewer a test device with each solution's test environment. This will again, reduce any bias that could be introduced by reviewing the solutions on different systems, with different settings.

The overall methodological approach assumes that each Bidder will be able to provide a test environment for their solution that is set up for each of the user tasks that have been identified above.

1.4 Stage 3: Reporting

The findings from both the heuristic evaluation and the summative usability tests will be compiled into a consolidated report card for each solution. The average weighted ratings and the performance along each of the usability metrics will be used to provide an overall assessment of each solution. In addition, the observations and discussions following the usability tasks will also provide additional insight into the performance of each solution.

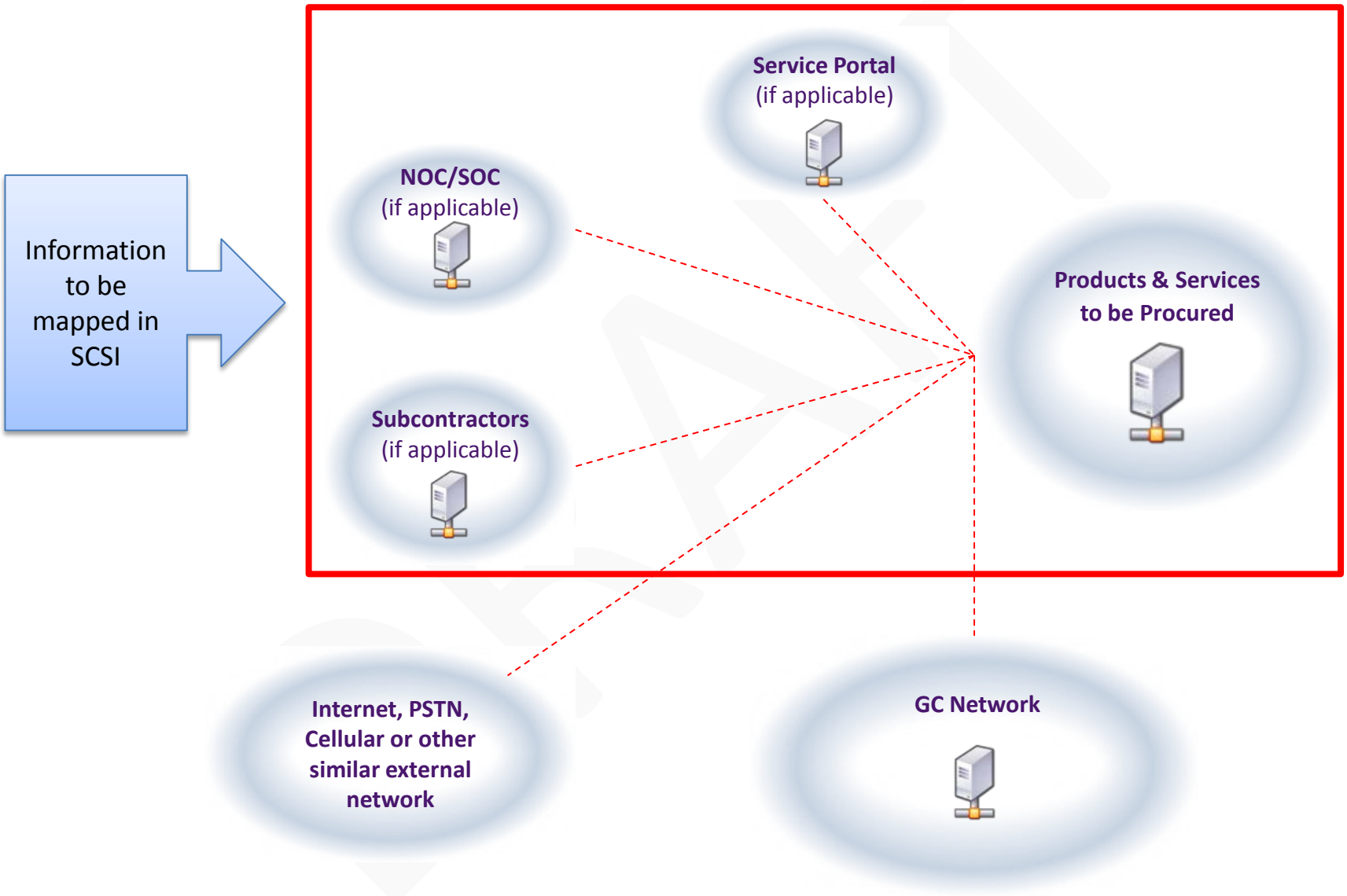
The methodology is not meant to have participants compare their experiences across the different platforms (as they will not be exposed to all tasks and all solutions). Rather, the metrics gathered across all of the 30 interviews combined with the outcomes of the heuristic assessment will benchmark performance.

To avoid any potential misinterpretation, metrics will be presented in the final report as counts (e.g. 8/12 were able to successfully complete User Task 1 on Solution X).

ATTACHMENT 4 TO PART 4:

SUPPLY CHAIN SCOPE DIAGRAM

Supply Chain Scope Diagram



ATTACHMENT 5 TO PART 4:

FINANCIAL EVALUATION

Attachment 5 to Part 4 – Financial Evaluation

A. EPS Transition-In Fee

	Expressed as a Firm Lump Sum Fee in Canadian dollars, custom duties included, Applicable Taxes are extra	
For the entirety of the Work described in Part 6, section 6.3 to 6.5 of the Statement of Work in Annex 1. ***Cannot exceed $750.000.00.**	$0.00	

Total for A - EPS Transition-In Fee	$0.00

B. EPS Operational Fee

	Expressed as a Monthly Lump Sum Fee in Canadian dollars, custom duties included, Applicable Taxes are extra	Multiplied by 12 months	Annual amount	Estimated usage for the entire length of the Contract (in years) - FOR EVALUATION PURPOSES ONLY	Sub-Totals
Tier 1: 1 to 5,000 Users **For all authorized Work in accordance with all sections of the Statement of Work in Annex 1, with the exception of Part 6, section 6.3 to 6.5 and Part 7.**	$0.00	12	$0.00	5	$0.00

	Expressed as a Firm Monthly Rate per User in Canadian dollars, custom duties included, Applicable Taxes are extra	Multiplied by 12 months	Annual amount	Estimated usage per year (in # of Users) - FOR EVALUATION PURPOSES ONLY	Extended annual amount	Estimated usage for the entire length of the Contract (in years) - FOR EVALUATION PURPOSES ONLY	Sub-Totals
Tier 2: in excess of 5,000 Users **For all authorized Work in accordance with all sections of the Statement of Work in Annex 1, with the exception of Part 6, section 6.3 to 6.5 and Part 7.**	$0.00	12	$0.00	2,500	$0.00	5	$0.00

	Expressed as a Monthly Lump Sum Fee in Canadian dollars, custom duties included, Applicable Taxes are extra	Multiplied by 12 months	Annual amount	Estimated usage for the entire length of the Contract (in years) - FOR EVALUATION PURPOSES ONLY	Sub-Totals
Tier 3: unlimited Users **For all authorized Work in accordance with all sections of the Statement of Work in Annex 1, with the exception of Part 6, section 6.3 to 6.5 and Part 7.**	$0.00	12	$0.00	7	$0.00

Total for B - EPS Operational Fee	$0.00

C. Optional Services Fees

Optional Work	Expressed as a Fixed Price in Canadian dollars, custom duties included, Applicable Taxes are extra
For the Work described in section 7.2.3 – Tender Feeds of the Statement of Work in Annex 1.	$0.00
For the Work described in section 7.2.4 – Data Escrow of the Statement of Work in Annex 1.	$0.00
Total for Optional Work	$0.00

Professional Services Category	Level	Per Diem Rates	Estimated annual usage (in days) - FOR EVALUATION PURPOSES ONLY	Extended Amount	Multiplied by 12 Years	Sub-Totals
A.1 Application/Software Architect	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
A.6 Programmer/Software Developer	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
A.8 System Analyst	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
A.12 WEB Architect	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
A.14 WEB Developer	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
I.1 Data Conversion Specialist	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
I.5 IM Architect	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
I.11 Technology Architect	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
B.1 Business Analyst	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
B.5 Business Process Re-engineering Consultant	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
B.7 Business Transformation Architect	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
P.1 Change Management Consultant	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
P.4 Organizational Development Consultant	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
C.3 IT Security TRA and C&A Analyst	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
C.6 IT Security Engineer	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
C.7 IT Security Design Specialist	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
C.8 Network Security Analyst	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
C.11 IT Security VA Specialist	Level 1	$0.00	20	$0.00	12	$0.00
	Level 2	$0.00	20	$0.00	12	$0.00
	Level 3	$0.00	20	$0.00	12	$0.00
					Total for Professional Services	$0.00

Total for C - Optional Services Fees	$0.00

TOTAL EVALUATED PROPOSAL PRICE **(in Canadian dollars, custom duties included, Applicable Taxes are extra)**	
Item	**Sub-Totals**
EPS Transition-In Fee	$0.00
EPS Operational Fee – Tier 1: 1 to 5,000 Users	$0.00
EPS Operational Fee – Tier 2: in excess of 5,000 Users	$0.00
EPS Operational Fee – Tier 3: Unlimited Users	$0.00
Optional Work – Fixed Prices	$0.00
Professional Services	$0.00
Total Evaluated Proposal Price	$0.00

FORM 1 TO PART 4:

RFP SUBMISISON FORM

1.0 RFP Submission Form

#	Response
	Bidder's full legal name
(a)	
	Bidder's Procurement Business Number
(b)	
	Authorized Representative of Bidder for evaluation purposes (e.g. clarifications)
(c)	Name:
	Title:
	Address:
	Telephone #:
	Email:
	If submitting a bid in response to the RFP as a joint venture, the Bidder must provide the joint venture member's full legal name and address [*Bidder to add more rows if more than two joint venture members*]
(d)	Joint venture member full legal name:
	Joint venture member address:
(e)	Joint venture member full legal name:
	Joint venture member address:
	RFP Submission Requirements It is the Bidder's sole responsibility to ensure their response addresses all requirements outlined in the RFP.

Bidder Authorization: On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that: 1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation; 2. This bid is valid for the period requested in the bid solicitation; 3. All the information provided in the bid is complete, true and accurate; and 4. 4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.	
(f)	Name:
	Address:
	Email:
	Signature of authorized representative of Bidder
	Phone:
	Date:
If submitting a bid in response to the RFP as a joint venture, the Bidder must complete section (g) below. [*Bidder to add more rows if more than two joint venture members*]	
(g)	Name:
	Address:
	Email:
	Signature of authorized representative of Bidder:
	Phone:
	Date:

FORM 2 TO PART 4:

PROJECT REFERENCE CHECK FORM

1.0 PROJECT REFERENCE CHECK FORM

Instructions to Bidders:

i. Bidders are requested to submit a Project Reference Check Form for each project referenced in response to each evaluation criteria in Attachment 2 to Part 4 of the RFP.
ii. If the information requested in this form is not provided with the Bidder's bid it must be provided upon request by the Contracting Authority within the timeframe identified in the request.
iii. Canada may contact the client contact, provided for the referenced project, to validate the information provided.

#	Response		
(a)	Evaluation Criteria Number (from Attachment 2 to Part 4)		
(b)	Bidder's Full Legal Name (if the Bidder is a joint venture, the full legal name of the joint venture member for the referenced project)		
(c)	Description of the referenced project		
(d)	Name of client organization for the referenced project		
(e)	Name of client contact for the referenced project		
(f)	Client organization and client contact affiliation with the Bidder (or joint venture member)		
	Please indicate accordingly	Are Not Affiliated	Are Affiliated
(g)	Name of organization the client contact is currently working for (if the client contact is no longer working for the client organization identified for the referenced project)		
(h)	Title of client contact (while working on the referenced project)		
(i)	Current telephone number of client contact		
(j)	Current e-mail address of the client contact		
(k)	Role of the client contact in the referenced project		

FORM 3 TO PART 4:

SCSI – IT PRODUCT LIST AND SUBCONTRACTOR LIST FORM

e-Procurement Solution

Bidder Name:	

Form 3 to Part 4 - (A) IT Product List

Line Item #	Location (a)	Product Type (b)	IT Component (c)	Product Acquisition Date (MM/YYYY or Undetermined future date) (d)	Model Name/ Number (e)	Description and Purpose (f)	Product Manufacturer and/or Software Publisher (g)	Name of Subcontractor (if equipment is being provided by a subcontractor) (h)
0								
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

Form 3 to Part 4 - (B) Subcontractor List

Solicitation No.: EN578-131350/xxx		Bidder's Legal Name:	
Name of the Subcontractor (a)	Address of the Subcontractor's headquarters (b)	Portion of the Work that would be performed by the Subcontractor (c)	Location(s) where the Subcontractor would perform the Work (d)

This page left blank intentionally.