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 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 - Proof of Proposal (PoP) Test
Attachment 4 to Part 4 – Supply Chain Network Diagram

List of Attachments to Part 6 of the RFP:
Attachment 1 to Part 6 – Service Level Agreements - Security & Privacy

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.

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 Contents for the list of annexes, attachments and forms.

1.2 Summary

1.2.1 Public Works and Government Services Canada is acquiring, on behalf of the Government of Canada, an Electronic Procurement Solution (EPS) to modernize public procurement practices so that they are simpler, less administratively burdensome and deploy modern comptrollership. In order to achieve this objective, the EPS must:

a) Achieve better value for Canadians through improved procurement outcomes;
b) Improve client service by providing easy, web-based access to procurement information and services to Departments and Agencies;
c) Provide easy, web-based access to information and services that reduce Supplier's burden of participating in the procurement process;
d) Achieve an integrated approach to the management of government spend; and
e) Enable procurement professionals with new tools, technology and processes to deliver effective client services.

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process, including their preliminary evaluation results, if applicable. 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. Bidders should note that they will only be advised whether they passed or failed the SCSI assessment. No other details will be provided on this portion of the evaluation.

1.4 Conflict of Interest

1.4.1 Bidders are advised to refer to Conflict of Interest provisions at section 18 of SACC 2003, Standard Instructions – Goods or Services – Competitive Requirements (dated 2016-04-04) and Conflict of Interest provisions of SACC 2035, General Condition – Higher Complexity – Services (dated 2016-04-04) 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	TRM Technologies Inc.
J3JTam Inc.	

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

Any bid that is received from one of the above-noted suppliers, whether as a sole Bidder, joint venture or as a sub-contractor to a Bidder; or for which one of the above-noted resources provided any input into the bid, will be considered to be in contravention of the Conflict of Interest clauses identified in subsection 1.4.1, and the bid will be declared non-responsive.

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 procurement. The Fairness Monitor will not be part of the evaluation team, but will, among other things, review all solicitation documents and observe the evaluation of the bid responses with respect to Canada's adherence to the evaluation process described in this RFP.

This RFP is a stand-alone procurement, independent of the Invitation to Qualify (ITQ) and the Review and Refine Requirements (RRR) process. The RFP contains the entirety of the requirements for the procurement, including the description of Work and evaluation criteria and procedures.

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 Guide (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 (2016-04-04) 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 days

2.1.5 The title of section 10 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, 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:

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

   ii. A list of all the Bidder's partners and/or major shareholders, 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

   iii. 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.

b. 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.

c. 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 RFP 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.

2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority, at the email address identified below, no later than 15 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 *section 2.3 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 volumes.

2.7 Bidders' Conference

A Bidders' conference will be held at Palais des Congrès at 50, boulevard Maisonneuve on May 3, 2016. The conference will begin at 10:00 EDT, in Room Desert A. The scope of the requirement outlined in the bid solicitation will be reviewed during the conference and questions will be answered. It is recommended that Bidders who intend to submit a bid attend or send a representative.

Bidders are requested to communicate with the Contracting Authority before the conference to confirm attendance. Bidders should provide, in writing, to the Contracting Authority, the name(s) of the person(s) who will be attending and a list of issues they wish to table no later than April 29, 2016.

Any clarifications or changes to the bid solicitation resulting from the Bidders' conference will be included as an amendment to the bid solicitation. Bidders who do not attend will not be precluded from submitting a bid.

2.8 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**"):

2.8.1 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.

2.8.2 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.

2.8.3 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 section, accesses the Sensitive Information at any time.

2.8.4 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.

2.8.5 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.

2.8.6 This Non-Disclosure Agreement remains in force indefinitely.

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:

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

ii. Section II: Technical Bid (6 hard copies and 1 soft copy on a USB in a format accessible by Canada) (can be on the same USB as Section I: SCSI)

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

iv. 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)

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

vi. Prices should appear in the financial bid only. Prices should not be indicated in any other Section of the bid.

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

viii. 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.

3.1.3 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.

3.1.4 Submission of Only One Bid from a Bidder

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 ask the Bidder to clarify which of the bids received from that Bidder is to be evaluated by Canada. Canada will only evaluate one bid per Bidder. However, Bidders may submit a bid as a sole Bidder and/or as a Joint Venture, or more than one Joint Venture, as long as the parties comprising each Joint Venture are not the same.

3.1.5 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 (2016-04-04) 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.

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 SCSI Assessment identified in Part 4, subsection 4.2.1.

3.2.2 The SCSI should include submission of Form 3 to Part 4 – SCSI - IT Product List and Subcontractor List Form, as well as the Network Diagram (refer to example in Attachment 4 to Part 4) 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 requirements contained in the bid solicitation. 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 the Bidder's response to Attachment 2 to Part 4 – Technical Evaluation, Form 1 and Form 2, 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 as per subsection 4.2.1

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

3.4 Section III: Financial Bid

3.4.1 Bidders must submit their Financial Bid in accordance with Annex 3 – Price Schedule.

3.4.2 Bidders Financial Bids must address each of the cost elements specified in this RFP. The Bidder should 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 will prevail. The quoted prices should be entered into the applicable cells of the Financial Evaluation only.

3.4.3 **All Costs to be included**: The Financial Bid includes all costs for the requirements described in the bid solicitation including any services in excess of the Statement of Work identified in the Contractor's bid response, for the entire Term of the Contract 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:** For tables 1, 2, 4, 5.1 and 6.1 in Annex 3 – Price Schedule, Bidders are requested to insert "$0.00" for any of the items for which it does not intend to charge or for items that are already included in other prices set out in the tables 1, 2, 4, 5.1, and 6.1. If any cost element in tables 1, 2, 4, 5.1, or 6.1 is left blank after *Step 2 – Final Evaluation of the Financial Mandatory Criteria (MFC 1)*, Canada will insert "$0.00" for that element. Bidders must quote an all-inclusive fixed daily rate for all levels and all categories of professional services listed in Table 3 of Annex 3 – Price Schedule. Blank Prices will not be accepted for professional services.

3.5 Section IV: Certifications

Bidders must submit the certifications and additional information 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 should 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

The information listed above should be submitted with the bid but may be submitted afterwards. If any of the information is missing, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the requested information within the time frame specified will render the bid non-responsive.

3.6.2 The Company Security Officer (CSO) should 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.

PART 4 - EVALUATION PROCEDURES

Notice to Bidders: Taking into consideration feedback received during the Review and Refine Requirements (RRR) process, the RFP mandatory technical criteria are derived from, but not the same as, the mandatory technical criteria from the Invitation to Qualify (ITQ). These criteria are independent of the ITQ and all Bidders must respond to all RFP mandatory technical criteria (refer to Attachment 2 to Part 4) of this RFP.

4.1 Evaluation Procedures

4.1.1 Bids will be assessed in accordance with the entire requirement of the bid solicitation.

4.1.2 An evaluation team of government representatives will evaluate the bids on behalf of Canada. The evaluation team will include PWGSC representatives and may include client department representatives or others designated by Canada. Canada may retain any independent consultant or use any government resources to evaluate any bid or bid portion thereof. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

4.1.3 The evaluation and selection will be conducted in multiple steps described below. The fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed any or all other steps. Canada reserves the right to conduct steps of the evaluation in parallel or in a different sequence than they appear in this RFP.

4.1.4 WGSC 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

4.1.5 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 as specified in the request. Failure to meet this deadline will result in the bid being declared non-responsive. If additional time is required by the Bidder, the Contracting Authority may grant an extension at his or her sole discretion.

4.1.6 Nothing in the bid evaluation process shall limit Canada’s rights under SACC 2003 (2016-04-04) Standard instructions – Goods or Services – Competitive Requirements nor Canada’s right to request or accept any information during the solicitation period or after bid solicitation closing in circumstances where the bid solicitation expressly provides for this right.

4.1.7 Where Canada has made a final determination that a bid has failed any individual mandatory element of the RFP, including a technical evaluation pass mark, Canada reserves the right to not proceed further in the evaluation of the bid and may deem the bid non-responsive.

4.2 Bid Evaluation

4.2.1 Section I: Supply Chain Security Information (SCSI) Assessment

4.2.1.1 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 SCSI. 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 bid or comes from another source, that Canada considers necessary to conduct a comprehensive assessment of the SCSI.

4.2.1.2 If, in Canada's opinion, any aspect of the SCSI, 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 (by email) and identify which aspect(s) of the SCSI 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 SCSI.

b. The notice will provide the Bidder with one opportunity to submit revised SCSI 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. However, a Bidder may choose to withdraw from the evaluation instead of revising its SCSI.

d. If the Bidder submits revised SCSI within the allotted time, Canada will perform a second assessment. If Canada determines that any aspect of the Bidder's revised SCSI could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, no further opportunities to revise the SCSI will be provided and the bid will be deemed non-responsive.

4.2.1.3 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 SCSI has become the subject of security concerns. At that point, Canada may notify the Bidder and provide the Bidder with an opportunity to revise its SCSI, using the same process described above.

b. during the performance of the resulting contract, if Canada has concerns regarding certain products, designs or subcontractors originally included in the SCSI, the terms and conditions of that contract will govern the process for addressing those concerns.

4.2.1.4 Once a Bidder has passed the SCSI Assessment, no modifications are permitted to the SCSI except as circumstances require, 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.

Notice to Bidders for subsections 4.2.2 and 4.2.3: The two step processes, outlined below, involve preliminary evaluations of the technical and financial bids to help identify non-compliancy and provide a fair and transparent process for all Bidders to revise their bid subject to the conditions described herein. Through these two step processes, Canada wishes to obtain competitive and thoroughly assessed bids as well as a fair process by permitting revisions, including administrative bidding errors by a Bidder against the mandatory elements as described herein.

4.2.2 Section II: Technical Bid Evaluation

Canada will conduct the evaluation of the Technical Bid in two steps.

4.2.2.1 Step 1 – Preliminary Technical Evaluation

A Preliminary Technical Evaluation will be conducted first, in accordance with *section 6 of Attachment 1 to Part 4.*

4.2.2.2 Step 2 – Final Technical Evaluation

Final Technical Evaluation: Step 2 of the technical bid evaluation – the Final Technical Evaluation – will occur after Step 1. Where a bid has passed all the mandatory technical criteria, including point-rated criteria pass marks in the Preliminary Technical Evaluation, the evaluation team will affirm that the Preliminary Technical Evaluation conducted in step 1 will be the Technical Bid Evaluation results for that bid. However, where a bid has failed one or more of the mandatory requirements in the Preliminary Technical Evaluation, including any point-rated criteria pass marks, or the Bidder added a bid condition, the second step will be conducted for that bid(s) as described below.

4.2.2.3 Canada Provides Preliminary Technical Evaluation Result: Canada will only advise the Bidder as to which mandatory technical criteria or point-rated criteria pass mark, it failed in the Preliminary Technical Evaluation. To ensure fairness to all Bidders, Canada will not provide a debriefing on their Preliminary Technical Evaluation results nor further detail on these evaluation results as part of step 2.

4.2.2.4 Bidder Submits Technical Bid Revision: The Bidder will be invited to submit a bid revision to its Technical Bid only, and/or remove any bid conditions if applicable, in response to the mandatory technical criteria and/or point-rated criteria pass marks identified as failed by Canada. Where the addition of such information will necessarily result in a change to the information it submitted in response to other mandatory or point-rated criteria as part of its Technical Bid, the Bidder must identify the affected criteria and only these adjustments should be made.

4.2.2.5 Any other changes to the bid shall be considered new information and will not be considered by the evaluators in the Final Technical Evaluation unless the evaluation team determines, in accordance with the evaluation criteria, that it has a negative impact on any of the preliminary scores the evaluation team had assigned in the Preliminary Technical Evaluation. If this is the case, to preserve fairness amongst all Bidders and to ensure Canada is protected, the evaluators shall evaluate the applicable technical criteria in light of this new information and may reduce, but not increase, the score of any applicable point-rated criteria. This new score will be reflected in the Final Technical Evaluation result of step 2.

4.2.2.6 Technical Bid Evaluation Result: The bid revisions submitted by the Bidder in step 2 will be used in the technical evaluation to determine whether or not the Bidder passed the mandatory technical criteria and the point-rated criteria pass marks. For the point-rated criteria, the new evaluated point score in step 2 would not be used in the determination of the Bidders Technical Score. The technical evaluation score that would be used to determine the Technical Score would be the evaluation score for that criterion as determined in the Preliminary Technical Evaluation in step 1 (less any applicable technical criteria reductions as described in subsection 4.2.2.5, above.)

4.2.2.7 Additional Restrictions: Without limiting the foregoing, the Bidder must not make any changes to the Financial Bid as a result of any changes through its Technical Bid revision. Should the Bidder introduce changes to the Financial Bid through the above process, it will be given one opportunity to withdraw the financial changes. Failure to withdraw the changes will result in its bid being declared non-responsive and no longer considered by Canada.

4.2.2.8 In Step 2, Canada will complete Final Technical Evaluation, in accordance with the process described in *section 6 of Attachment 1 to Part 4*.

4.2.3 Section III: Financial Bid Evaluation

4.2.3.1 Evaluation of Mandatory Financial Criteria 1 (MFC 1)

4.2.3.1.1 *Step 1 – Preliminary Evaluation of the Mandatory Financial Criteria (MFC 1)*

Canada will conduct the evaluation of the Financial Bid for MFC 1 in two steps. A Preliminary Evaluation of the financial mandatory criteria MFC 1 will be conducted first in accordance with *section 7 of Attachment 1 to Part 4*.

4.2.3.1.2 Step 2 – Final Evaluation of the Financial Mandatory Criteria (MFC 1)

Final Evaluation of the Financial Mandatory Criteria (MFC 1): Step 2 of the Financial Bid Evaluation – the Final Evaluation of the Financial Mandatory Criteria (MFC 1) – will occur after Step 1. Where a bid has passed the mandatory financial criteria MFC 1, as identified in *Attachment 1 to Part 4 – Evaluation and Selection Methodology, subsection 7.1*, the financial evaluation team will affirm that the Preliminary Evaluation of the mandatory financial criteria MFC 1 conducted in step 1 will be the final Financial Bid Evaluation result for that bid for the mandatory financial criteria MFC 1. However, where a bid has failed the mandatory financial criteria MFC 1, the second step will be conducted for that bid(s) as described below.

4.2.3.1.3 Canada Provides Preliminary Evaluation of the Mandatory Financial Criteria MFC 1 Result: Canada will advise the Bidder that it failed mandatory financial criteria MFC 1 in the preliminary financial mandatory criteria MFC 1 evaluation. To ensure fairness to all Bidders, Canada will not provide a debriefing on these evaluation results nor provide further details on these evaluation results.

4.2.3.1.4 Bidder Submits Financial Bid Revision: The Bidder will be invited to re-submit a revision to their Financial Bid to revise elements in their Financial Bid in response to mandatory financial criteria MFC 1.

4.2.3.1.5 In Step 2, Canada will complete final financial evaluation of MFC 1, in accordance with the process described in *section 7 of Attachment 1 to Part 4*.

4.2.3.2 Evaluation of Mandatory Financial Criteria 2 to 9 (MFC 2 – MFC 10)

4.2.3.2.1 Step 1 – Preliminary Evaluation of the Mandatory Financial Criteria (MFC 2 – MFC 10)

Canada will conduct the evaluation of the Financial Bid for MFC 2 to MFC 10 in two steps. A Preliminary Evaluation of the financial mandatory criteria MFC 2 to MFC 10 will be conducted first in accordance with *section 7 of Attachment 1 to Part 4*.

4.2.3.2.2 Step 2 – Final Evaluation of the Financial Mandatory Criteria (MFC 2 – MFC 10)

Final Evaluation of the Financial Mandatory Criteria: Step 2 of the Financial Bid Evaluation – the Final Evaluation of the Financial Mandatory Criteria (MFC 2 – MFC 10) – will occur after Step 1. Where a bid has passed all the mandatory financial criteria, as identified in *Attachment 1 to Part 4 – Evaluation and Selection Methodology, subsection 7.1*, the financial evaluation team will affirm that the Preliminary Evaluation of the Mandatory Financial Criteria conducted in step 1 will be the final Financial Bid Evaluation result for that bid for the mandatory financial

criteria. However, where a bid has failed one or more of the mandatory financial criteria, the second step will be conducted for that bid(s) as described below.

4.2.3.2.3 Canada Provides Preliminary Evaluation of the Mandatory Financial Criteria MFC 2 to MFC 10 Result: Canada will advise the Bidder as to which mandatory financial criteria they failed in the preliminary financial mandatory criteria evaluation. To ensure fairness to all Bidders, Canada will not provide a debriefing on these evaluation results nor provide further details on these evaluation results.

4.2.3.2.4 Bidder Submits Financial Bid Revision: The Bidder will be invited to re-submit a revision to their Financial Bid to revise elements in their Financial Bid in response to these mandatory requirements identified by Canada.

4.2.3.2.5 In Step 2, Canada will complete final financial evaluation, in accordance with the process described in *section 7 of Attachment 1 to Part 4*.

4.2.4 Additional Responsibilities for Steps 1 and 2 of the Technical and Financial Bid Evaluations

4.2.4.1 Bidders are and will remain solely responsible for the accuracy and completeness of their bids and Canada does not undertake, by reason of the step 1 preliminary technical and financial mandatory criteria evaluations, any obligations or responsibility for identifying errors or omissions in bids submitted nor does Canada undertake to identify any or all such errors or omissions.

4.2.4.2 Bidders are and will remain solely responsible for ensuring consistency of the information submitted in their bids at all times. Without limiting the foregoing, Bidders are and will remain solely responsible for ensuring that any information provided in response to a preliminary technical or financial mandatory criteria evaluation is consistent with any other information originally submitted in their bid in response to other requirements. Failure to do so may prejudice the evaluation of previously submitted information and/or render the bid non-responsive.

4.2.5 Bid revisions must follow the Bid Preparation Instructions (such as, for example, separating financial information from other information as required). Canada requests that Bidders clearly indicate, for each bid revision, which non-responsive requirement is being responded to.

4.2.6 Bid revisions must be submitted by email to the Contracting Authority within 5 business days (or longer period if specified in writing by the Contracting Authority). Failure to do so will result in the bid being deemed non-responsive and the bid will receive no further consideration.

4.2.7 The changes within any bid revision are at the Bidder's sole discretion and will be made solely by the Bidder. Canada will not provide information about any other bid or any information as to how a Bidder should prepare the content of its bid revision.

4.2.8 For those instances where a Bidder chooses not to submit additional or different information for a requirement identified as non-responsive or as having not achieved the minimum score for a point-rated criteria, the Bidder must submit a response indicating "No Change" for such requirement and the original response for that item will continue to apply. If a Bidder does not provide a "No Change" response, the Bidder shall be deemed to have provided a "No Change" response and the original bid response for that item shall continue to apply.

4.2.9 In addition to any other obligations contained in the resulting contract, the winning Bidder will be contractually obliged to provide all services described in its bid and bid revisions in responses to Attachment 2 to Part 4 – Technical Evaluation where it has been awarded technical points for such bid and bid revisions, 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 Bidder selected by Canada must deliver the requested services in accordance with the Resulting Contract.

4.2.10 Bidders will not be allowed to change the composition of the Bidder's team (i.e. a Bidder cannot add or withdraw any team members, including subcontractors, when submitting revised information). Any change to the composition of the Bidder will result in the bid being declared non-responsive.

PART 5 - CERTIFICATIONS

Bidders must provide the required certifications and additional 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 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 Term of the Contract.

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 will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information 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 provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.1.1 Integrity Provisions - List of Names

Bidders who are incorporated, including those bidding as a Joint Venture, must provide a complete list of names of all individuals who are currently directors of the Bidder.

Bidders bidding as sole proprietorship, as well as those bidding as a Joint Venture, must provide the name of the owner(s).

Bidders bidding as societies, firms or partnerships do not need to provide lists of names.

5.1.2 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 Term of the Contract.

The Bidder must provide the Contracting Authority with a completed Federal Contractors Program for Employment Equity certification before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority before contract award with a completed Federal Contractors Program for Employment Equity certification for each member of the Joint Venture. Form 1 to Part 4 – RFP Submission Form, includes a copy of the certification.

5.2 Additional Certifications Precedent to Contract Award

Refer to Form 1 to Part 4 – RFP Submission Form for all additional certifications that must be submitted precedent to Contract award.

PART 6 – SECURITY AND FINANCIAL REQUIREMENTS

6.1 Security Requirements

On or before Contract award, 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. The **Contractor** and any and all **subcontractors** must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) 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, as updated from time to time.

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 Bidder must provide proof that it is incorporated or authorized to do business in its jurisdiction as indicated in Part 7 - Resulting Contract Clauses, 7.5 B.,b. Security Requirement for Foreign Suppliers.

iv. The Bidder 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 or where the local legislation requires such registration

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

v. The Bidder will need to provide assurance that it can safeguard, manage and protect all Personal Information as indicated in Part 7 – Resulting Contract Clauses, *Section 7.5 Security Requirements.*

vi. The bid should clearly indicate the work which the Bidder plans to subcontract. All subcontracting arrangements which provide the subcontractor with access to any Personal Information are subject to approval by Canada. The description of subcontracting arrangements should demonstrate how the Bidder will ensure that all requirements, terms, conditions, and clauses of the contract are met.

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

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); and 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.*

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 Security Information (SCSI) Assessment Definitions

The following words and expressions used in the Supply Chain Security Information Assessment have the following meaning:

a. "Products" means any hardware that operates at the data link layer of the Open Systems Interconnection (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 requested to be done, delivered or performed by the Contractor under the resulting Contract.

7.3 Task Authorization

A. Work described at part 7 of Annex 1 – Statement of Work, will be performed under the Contract on an “as and when requested basis”.

B. With respect to the Work mentioned under paragraph A of this clause,

1. an obligation will come into force only when the Contractor receives a Task Authorization (TA), inclusive of any revisions, authorized and issued in accordance with this clause, and only to the extent designated in the authorized TA;

2. the TA Authority and limit will be determined in accordance with paragraph C of this clause;

3. the Contractor must not commence work until a TA, or any TA revisions thereof, has been authorized and issued in accordance with the Contract. The Contractor acknowledges that work performed before a TA or revision of a TA, has been authorized and issued in accordance with the Contract will be done at the Contractor’s own risk and expense;

4. the task description, included in an authorized TA must fall within the scope of part 7.0 of the Statement of Work, in Annex 1*;* and

5. the TA, or any TA revisions thereof, will be authorized under the Contract through the use of Annex 7 – Task Authorization Form. An authorized TA is a completed Annex 7 – Task Authorization Form signed by the TA Authority.

C. TA Authority and Limit

The Project Authority may authorize individual TAs inclusive of any revisions up to a limit of $100,000.00, Applicable Taxes extra. Any TA, the total value of which would exceed that limit, or any revision to a previously authorized TA that would increase the TA total value above that limit, must be authorized by the Contracting Authority before issuance to the Contractor.

D. The authority specified under paragraph C of this clause is granted subject to the sum specified in the Contract in subsection *7.10.2 Limitation of Expenditure – Portion of the Work – Cumulative Total of all Authorized TAs* not being exceeded.

E. TA Process

For each task or revision of a previously authorized task, the Project Authority will provide the Contractor with a request to perform a task prepared using Annex 7 – Task Authorization Form, containing as a minimum:

- the task or revised task description of the Work requested, including:
  - the details of the activities or revised activities to be performed;
  - a description of the deliverables or revised deliverables to be submitted; and
  - a schedule or revised schedule indicating completion dates for the major activities or submission dates for the deliverables, or both, as applicable;
- the Contract security requirements applicable to the task or revised task;
- the Contract basis (bases) of payment applicable to the task or revised task; and
- the Contract method(s) of payment applicable to the task or revised task and, as applicable, the associated schedule of milestones.

F. Within 5 calendar days of its receipt of the request, the Contractor must provide the Project Authority with a signed and dated response prepared and submitted using the TA form received from the Project Authority, containing as a minimum:

1. the total estimated cost proposed for performing the task or, as applicable, revised task;
2. a breakdown of that cost in accordance with Annex 3 – Price Schedule, to be provided, as applicable, per milestone contained in the Schedule of Milestones; and
3. for each resource proposed by the Contractor for the performance of the Work requested:
   - the name of the proposed resource;
   - the resume of the proposed resource; and
   - a demonstration that the proposed resource meets:
     - the Contract security requirements; and
     - the requested experience identified in subsection 7.1.3 of the SOW.

The above applies only to TAs where Canada will pay for Work that is not otherwise covered by fixed fees in the Contract (i.e. EPS Transition-In Firm Lot Price and EPS Operational Firm Lot Monthly Price).

G. TA Authorization

1. The TA Authority will authorize the TA based on:

   - the request submitted to the Contractor pursuant to paragraph E of this clause;
   - the Contractor's response received, submitted pursuant to paragraph F of this clause; and
   - the agreed total estimated cost for performing the task or, as applicable, revised task; and, as applicable, the breakdown of that cost per milestone.

2. The TA Authority will authorize the TA provided each resource proposed by the Contractor for the performance of the Work requested meets all the requirements specified under paragraph F.3 of this clause.

3. The authorized TA will normally be issued to the Contractor by email (i.e. as an email attachment in PDF format).

H. Periodic Usage Reports - Contracts with TAs

1. The Contractor must compile and maintain detailed and current data on its performance of Work required and requested under TAs (inclusive of any revisions) authorized and issued under the Contract.

2. No later than 15 calendar days after the end of each of the reporting periods below, the Contractor must submit to the Contracting Authority and Project Authority a Periodic Usage Report containing, in an electronic spreadsheet (such as MS Office Excel), the data elements specified in paragraphs J.3 and J.4 of this clause in the order they are presented. Where at the end of a reporting period, no changes are required to be made to the data contained in the periodic usage report submitted for the previous period, the Contractor must submit a "NIL" report to the Contracting Authority and Project Authority.

The reporting 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.

3. For each TA authorized and issued under the Contract, the Periodic Usage Report must include the following data elements in the order presented:

- the TA number appearing on the TA form;
- the date the task was authorized appearing on the TA form;
- the total estimated cost of the task (Applicable Taxes extra) before any revisions appearing on the TA form;
- the following information appearing on the TA form must be included for each authorized revision, starting with revision 1, then 2, etc.;
- the TA revision number;
- the date the revision to the task was authorized;
- the authorized increase or decrease (Applicable Taxes extra);
- the total estimated cost of the task (Applicable Taxes extra) after authorization of the revision;
- the total cost incurred for the task (as last revised, as applicable), Applicable Taxes extra;
- the total cost incurred and invoiced for the task (as last revised, as applicable), Applicable Taxes extra;
- the total amount of Applicable Taxes invoiced;
- the total amount paid, Applicable Taxes included;
- the start and completion date of the task (as last revised, as applicable); and
- the active status (i.e., the percentage of the work completed) of the task (as last revised, as applicable) with an explanation (as applicable).

4. For each TA authorized and issued under the Contract, the Periodic Usage Report must include the following data elements in the order presented:

- the total cost incurred for all authorized tasks inclusive of any revisions, Applicable Taxes extra;
- the total cost incurred and invoiced for all authorized tasks inclusive of any revisions, Applicable Taxes extra;
- the total amount of Applicable Taxes invoiced for all authorized tasks inclusive of any revisions; and
- the total amount paid for all authorized tasks inclusive of any revisions, Applicable Taxes extra.

I. 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.

J. 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 authorized tasks performed by the Contractor.
b. Canada reserves the right, at any time, to acquire the requested Work by other means including to select other suppliers. For example, Canada may decide to acquire the requested Work by other means when the Contractor provides a written proposal that has been rejected by Canada.

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 (2016-04-04), 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 section entitled "Replacement of Specific Individuals" in its entirety.
(ii) Insert section 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-paragraph 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 section apply despite any changes that Canada may have made to the Client's operating environment.

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

   i. The general conditions are amended by deleting in its entirety the section entitled "Copyright", and replacing it with the following:

"Without affecting any existing intellectual property rights or relating to information or data supplied by Canada for purposes of the Contract, copyright in anything conceived, developed, or produced as part of the Work under the Contract will belong to the Contractor."

ii. K3030C (2010-01-11), License to Material Subject to Copyright apply to and form part of the Contract

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 and performing the Work listed and described in the Contract. These security requirements are in addition to those requirements already identified in Part 7 - Resulting Contract Clauses, *section 7.5.1 Protection and Security of Data Stored in Databases For Canadian and Foreign Suppliers*, *section 7.5.2 - Privacy and Personal Information*, and Annex 2 - Security and Privacy Requirements.

a. The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening , 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 **RELIABILITY STATUS**, 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, PWGSC, 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 legislation of 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 Data Protection Authority (DPA) and the Contracting Authority and Project Authority (in collaboration with the Canadian Designated Security Authority (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 PWGSC. Further information on the responsibilities of a Company Security Officer (CSO) and instructions on completing the form can be found at: http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html

B. SECURITY REQUIREMENTS FOR FOREIGN SUPPLIERS:

The Canadian Designated Security Authority (Canadian DSA) for industrial matters in Canada is the Industrial Security Sector (ISS), 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 the Contract. These security requirements are in addition to those requirements already identified in Part 7 – Resulting Contract Clauses, *section 7.5.1 Protection and Security of Data Stored in Databases For Canadian and Foreign Suppliers, section 7.5.2 - Privacy and Personal Information* and Annex 2. 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 and any and all subcontractors must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) 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, and as updated from time to time.

b. The Contractor must be registered with the appropriate government supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or authorized to do business and operating or where the local legislation requires such registration.

c. The Contractor will need to provide assurance that it can safeguard, manage, and protect all Personal information.

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 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 must 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 and/or the NSA/DSA of their country as well as a background verification. The approved verifications for the required criminal record check and background verification are listed at 7.5.3.

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

   iv. The Foreign Contractor must 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. The Contractor and 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.

h. All Personal Information, provided to the Contractor and any and all subcontractors or produced by the Contractor and 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).

i. The Contractor and 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 have been lost, or in contravention of these security requirements, used or disclosed.

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

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

l. 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.

m. The Contractor visiting Canadian Government, under this Contract, must submit a Request for Visit form to the Departmental Security Officer of PWGSC.

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

a. The Contractor and any and all subcontractors must ensure that all the databases used by organizations to provide the Work described in the Contract containing any Personal

Information, related to the Work, are located in a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) 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, and as updated from time to time.

b. The Contractor and any and all subcontractors must control access to all databases, referred to in paragraph 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 any and all subcontractors must not subcontract (including to a parent, subsidiary or affiliate) any function, relating to the provision of Work described in –the Contract, 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.

7.5.2 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, including Annex 4 - Security Requirements Check List (SRCL) and Security Classification Guide (SCG).

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 4 - Security Requirements Check List (SRCL) and Security Classification Guide (SCG) and the 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.

7.5.3 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 which must include the following elements:

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. Gender
   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
xii. The last five 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
xiii. The educational establishments attended and the corresponding dates.

d. Employment history check
xiv. The last five years of employment history starting from most recent with no gaps in time.
xv. Three employment reference checks from the last five years.

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

7.6 On-going Supply Chain Security Information (SCSI) Assessment

7.6.1 Supply Chain Security Information Assessment: The Contractor acknowledges that a Supply Chain Security Information Assessment was a key component of the procurement process that resulted in the award of this Contract. In connection with that assessment, Canada assessed the Contractor's 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 Contractor also acknowledges 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 Term of the Contract. This section 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 (not 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. This list of IT products does not need to include IT Products used within each subcontractor, unless requested by Canada.

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 necessary to conduct a comprehensive assessment of any proposed new SCSI.

e. Due to the Software-as-a-Service (SaaS) nature of this solution, the Contractor is required to provide only the Network Diagrams and List of Subcontractors details, rather than each IT product used by each subcontractor. However, if specific supporting IT products are to be used by the Contractor itself, those details must be provided.

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 Term of the Contract.

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 SCSI assessment by Canada, but for which new security vulnerabilities have since been identified.

d. Despite the previous subsection, 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 requested 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 section 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 section 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 requested by Canada pursuant to this section 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 Project 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 requested by the Contracting Authority.

b. For the purposes of this section, 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.

c. Consent provided by Canada for a subcontractor does not in any way relieve the Contractor of any of its obligations under this Contract.

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 subsection, 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 information had a fiduciaryrelationship with one another (eiher 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 each 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 20 working days after any change of control takes place (or, in the case of a subcontractor, within 25 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 section, 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 for convenience by providing notice to the Contractor within 90 calendar 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 calendar 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 for convenience by providing notice to the Contractor within 180 calendar days of receiving the original notice from the Contractor regarding the change of control.

h. In this section, termination for convenience 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 for convenience 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 intend to terminate the contract pursuant to this section 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 section 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 5 years later.

7.7.2 Option to Extend the Contract

a. The Contractor grants to Canada the irrevocable option to extend the Period of the Contract by up to 7 additional 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 *Annex 3 – Price Schedule*.

b. Canada may exercise these options 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 confirmed 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

The Contractor's Representative and Executive Authority for the contract is: *(to be confirmed at contract award)*

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 Terms of Payment

7.10.1 Basis of Payment

(i) e-Procurement Solution Transition-In

For the entirety of the Work in the Statement of Work in Annex 1 relating to the Transition-in delivery, including *subsection 6.8 Transition Services* and the completion of all milestones described in *subsection 6.10 Milestones* and the entirety of the Work in Annex 2 – Security and Privacy, as consideration to the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor an EPS Transition-In Firm Lot Price detailed in Annex 3 – Price Schedule, customs duties included and Applicable Taxes extra. The EPS Transition-In Firm Lot Price is divided into milestones as set out in Annex 3 – Price Schedule. Each EPS Transition-In milestone amount is payable only after successful completion and acceptance by Canada of the respective milestone to which the milestone amount applies.

(ii) e-Procurement Solution Operational

The EPS Operational Firm Lot Monthly Price and Firm Unit Prices are consideration for all authorized Work in accordance with all sections of the Statement of Work with the exception of the Work covered under paragraph (i) above and Part 7 of the Statement of Work in Annex 1.

The EPS Operational Firm Lot Monthly Price is payable monthly and begins in the month subsequent to the successful completion (and Canada's acceptance) of milestones #1 & #2 of the EPS Transition-In phase. The amount of the EPS Operational Firm Lot Monthly Price is based on the progressive completion and acceptance by Canada of the EPS Transition- In milestones. Canada will increase the percentage of the Firm Lot Monthly Price to be paid to the Contractor, as set-out in Annex 3 – Price Schedule. Each applicable increase will take effect in the month subsequent to the Contractor's successful completion (and Canada's acceptance) of the applicable milestone.

The EPS Operational Firm Unit Prices are payable monthly for actual usage, beginning in the month subsequent to the successful completion (and Canada's acceptance) of milestones #1 & #2 of the EPS Transition-In phase. Canada will pay the Contractor the Firm Unit Price within the corresponding Tier as detailed in Annex 3 – Price Schedule for the following metric *(only one of the following metrics will be inserted at contract award – i.e., the metric below that is bid by the Bidder in their proposal)*:

_____ *(the metric)* is defined as:

Procurement Users – Users within the Government of Canada (employees and contracted resources of the GC) defined as Authorized Administrators and Authorized Users, not including Contractor resources, in accordance with Annex 5 – Glossary, and that have been granted access to the EPS functions for such users as described in the SOW.

GC Users – Users within the Government of Canada (employees and contracted resources of the GC) that are registered with an account and that are granted access to the EPS functions for such users as described in the SOW. The definition of GC Users does not include any accounts related to Suppliers, as defined in Annex 5 – Glossary, or Contractor resources.

Catalogue Spend – The total Canadian Dollar Value of Orders issued against Framework Agreements (Catalogues) in EPS. Catalogue Spend is calculated using the enumerated (i.e, stated in an explicit dollar figure) value of the Order. It does not include amounts that may be extra to the explicitly stated dollar figure of the Order such as taxes, shipping, duties, as applicable, unless these are included in the explicitly stated dollar figure of the Order. The total is net of any Order adjustments (positive and negative) made during the applicable period of measurement.

Transactions – Contracts and Orders awarded and Contract and Order amendments issued through EPS by GC Users or Procurement Users.

Note to Bidders: If the GC Users or Procurement Users metric is selected, the following will apply.

Canada will use the Monthly Firm Unit Price corresponding to the applicable tier based on the highest number of actual Users in that month. Canada will then pay that Monthly Firm Unit Price for each User in that month.

Note to Bidders: If the Catalogue Spend or Transactions metric is selected, the following will apply.

Annualizing the Catalogue Spend Metric or Transactions Metric – Tiers 1, 2, 3

The following will be used only for the Catalogue Spend Metric or the Transaction Metric, as applicable.

a.During the first 12 months of the EPS Operational, Canada will multiply the actual monthly volume by 12 to determine from which tier the Monthly Firm Unit Price will be used to determine the amount payable in that month.

b. Moving Annual Total (MAT)
For each month following the first 12 months of EPS Operational, the Moving Annual Total (MAT) will determine the applicable tier from which the Monthly Firm Unit Price will be selected and applied for payment in that month.

MAT is a method to convert a monthly volume into an annual volume for the purposes of determining which tier will be used for payment in that month. MAT is the total actual volume for the month in question, plus the sum of the actual volume for the previous 11 months for a total of 12 months.

MAT is a rolling yearly sum, so volumes at the end of each month are incorporated into the annual sum. For example, the MAT for the month of May 2019 would be the actual volumes from June 2018 to May 2019, inclusively. The MAT for June 2019 would be the actual volume from July 2018 to June 2019, inclusively.

Non-Cumulative Tiers

For all metrics, the monthly payment to the Contractor will be calculated using the rates within a single Tier. The Tiers are not to be applied in a cumulative fashion for any given month (i.e., if actual usage for the metric falls into Tier 2, the rates for Tier 2 will apply to the entire volume of usage for that month for that metric and the rates for Tier 1 do not apply. Similarly, if Tier 3 applies, it applies for the entire volume that month and the rates for Tier 1 and Tier 2 do not apply that month).

Annual Inflation Adjustment for EPS Operational Firm Lot Monthly Price and Firm Unit Prices
The Firm Lot Monthly Price and Firm Unit Prices for EPS Operational are subject to an annual inflation adjustment as of the first optional year of the Contract. 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 Firm Lot Monthly Price or Firm Unit Price. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

(iii) Optional Services

a. Professional Services provided under a Task Authorization

Using a Task Authorization (TA), for the Work described in subsection *7.1 – Optional Professional Services* and *7.2 Optional Defined Work*, with the exception of *7.2.4 Tender Feeds* and *7.2.6 Functional Requirements: Section F – Financial Management*, of the Statement of Work in Annex 1, and only where the Work is not otherwise covered by another section of the SOW, and for additional Work that may be added by Canada to Annex 1 – SOW and Annex 2 – Security and Privacy:

Professional Services provided under a Task Authorization: All Inclusive Fixed Daily Rates: For professional services, as and when requested by Canada during the Term of 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 Ceiling Price for the TA, for actual time worked and any resulting deliverables in accordance with the all-inclusive fixed daily rates in accordance with the prices included in Annex 3 – Price Schedule. 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.

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 all-inclusive fixed daily 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 Project Authority. All payments are subject to government audit.

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.

Annual Inflation Adjustment for Professional Services

The all-inclusive fixed daily rates for Professional Services are subject to an annual inflation adjustment as of April 1, 2018. 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 all inclusive fixed daily rates. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

b. Option for Tender Feeds

For the Work described in *subsection 7.2.4 – Tender Feeds* 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 a Firm Lot Price per feed in accordance with *Annex 3 – Price Schedule*, as specified in the authorized TA, customs duties included and Applicable Taxes extra.

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

Annual Inflation Adjustment for Firm Lot Price per Tender Feed

In the event that Canada does not exercise this optional service during the initial period of the Contract, the one-time Firm Lot Price per Tender Feed will be subject to an annual inflation adjustment as of the first optional year of the Contract. 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 Firm Lot Price. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

c. Option for Section F – Financial Management

Firm Lot Price per DFMS Instance for Financial Management Transition-In

For the entirety of the Work in subsection *7.2.6 – Functional Requirements: Section F – Financial Management* of the Statement of Work in Annex 1 relating to the Transition-In of Financial Management services for a DFMS instance:

As consideration to the Contractor for satisfactorily completing all of its obligations under the authorized Task Authorization (TA), Canada will pay the Contractor a Firm Lot Price per DFMS instance for Financial Management Transition-In for all the Work relating to the Transition-In of Financial Management services for a DFMS instance, as described in section *7.2.6 Functional Requirements: Section F – Financial Management*, in accordance with Annex 3 – Price Schedule and as specified in the authorized TA, customs duties included and Applicable Taxes extra. Each Firm Lot Price per DFMS Instance for Financial Management Transition-In amount is payable only after successful completion and acceptance by Canada of all the Work related to that DFMS instance.

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

Where Canada requests Financial Management services for more than one DFMS instance to be transitioned-in in the same request, the Firm Lot Price per DFMS instance for Financial Management Transition-In applicable in the request shall be discounted as follows:

Number of DFMS instances included in the request for Financial Management functionalities	Discount (reduction) applicable to each DFMS instance Financial Management Transition-In Firm Lot Price in the request
1	X%
2	X%
3	X%
4	X%
5-9	X%
10-15	X%
16 or more	X%

Annual Inflation Adjustment for Firm Lot Prices per DFMS instance for Financial Management Transition-In

In the event that Canada does not exercise this optional service during the initial period of the Contract, the one-time Firm Lot Prices for Financial Management Transition-In for each DFMS Instance will be subject to an annual inflation adjustment as of the first optional year of the Contract. 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 StatisticsCanada for the previous year. Any subsequent adjustments will be calculated on the most recent previous Firm Lot Price. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

d. DFMS Instance e-Procurement Solution Transition-In

For the entirety of the Work in the Statement of Work in Annex 1 relating to the Transition-in of a DFMS instance, including Annex 1 section 7.2.7, Government Wide Deployment, and the entirety of the Work in Annex 2 – Security and Privacy applicable to the interoperability with a DFMS instance, as consideration to the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor the applicable DFMS Instance EPS Transition-In Firm Lot Price detailed in Annex 3 – Price Schedule, customs duties included and Applicable Taxes extra. Each DFMS Instance EPS Transition-In amount is payable only after successful completion and acceptance by Canada of all the Work related to that DFMS instance.

Where Canada requests more than one DFMS instance to be deployed in the same request, the DFMS Instance EPS Transition Firm Lot Price applicable in the request shall be discounted as follows:

Number of DFMS Instances included in the request	Discount (reduction) applicable to each DFMS Instance EPS Firm Lot Price in the request
1	X%
2	X%
3	X%
4	X%
5-9	X%
10-15	X%
16 or more	X%

Annual Inflation Adjustment for DFMS Instance EPS Transition-In Firm Lot Price

In the event that Canada does not exercise this optional service during the initial period of the Contract, the one-time Firm Lot Prices for each DFMS Instance EPS Transition-In will be subject to an annual inflation adjustment as of the first optional year of the Contract. 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 Firm Lot Price. Where the CPI rate is a negative value, it will be treated as zero for the purposes of this adjustment.

e. Option for the Other Public Sector Entities:

(i) For the Work described in *subsection 7.3.1 – Extending Access to Other Canadian Broader Public Sector* Entities 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. Canada reserves the right to apply the PWGSC Contract Cost Principles 1031-2 as a basis for establishing the price of this Optional Work.

(ii) For the Work described in subsection *7.3.2 – Option for Other Canadian Broader Public Sector Entities to acquire a 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. Canada reserves the right to apply the PWGSC Contract Cost Principles 1031-2 as a basis for establishing the price of this Optional Work.

f. Option for the Broader Public Sector Tender Notices:

For the Work described in subsection *1.2.6 – Government Electronic Tendering Services (GETS)* of the *Statement of Work* in *Annex 1* pertaining to the posting of tender notices on GETS by the Canadian Broader Public Sector:

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 actual and reasonable cost, without allowance for profit, as specified in the authorized TA. Canada reserves the right to apply the PWGSC *Contract Cost Principles 1031-2* as basis for establishing the price of this Optional Work.

7.10.1.1 Competitive Award

The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges to the prices and rates specified in Annex 3 – Price Schedule will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

The Contractor further acknowledges that, due to the reporting limitations of the legacy systems currently in place, the volumetric data in this Contract is based on limited statistical information and are provided for information purposes only. The data is not to be considered as a contractual guarantee and may change during the Term of the Contract. No additional charges to the prices and rates specified in Annex 3 - Price Schedule will be allowed to compensate for volumetric changes unless expressly provided for in the Contract.

7.10.2 Limitation of Expenditure

A. With respect to the portion of the Work that is to be performed under the Contract on an "as and when requested basis" using Professional Services categories, Canada's total liability to the Contractor under the Contract for all authorized TAs, inclusive of any revisions, must not exceed the sum of $ _____ *(amount to be inserted at Contract award based on Canada's anticipated usage of Professional Services)*. Customs duties are included and the Applicable Taxes are extra.

B. No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

C. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

1. when it is 75 percent committed;

2. four (4) months before the contract expiry date; or

3. as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized TAs, inclusive of any revisions.

whichever comes first.

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

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

Canada will make milestone payments in accordance with the milestones detailed in Annex 3 – Price Schedule 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 requested by the Contracting Authority 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;
c. 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 – Firm Lot Monthly Price for e-Procurement Solution Operational

Canada will pay the Contractor, in arrears on a monthly basis and based on the milestones detailed in Annex 3 – Price Schedule, for the Work covered by the EPS Operational Firm Lot Monthly Price, if:

a. an accurate and complete invoice and any other documents requested by the Contracting Authority 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 to and accepted by Canada.

7.10.5 Method of Payment – Firm Unit Prices for e-Procurement Solution Operational

Canada will pay the Contractor, in arrears on a monthly basis and based on actual usage as detailed in Annex 3 – Price Schedule and section 7.10.1 (ii) above, for the Work covered by the EPS Operational Firm Unit Prices, if:

a. an accurate and complete invoice and any other documents requested by the Contracting Authority 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.

7.10.6 Method of Payment – Optional Services

For any TA using Professional Services categories 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, or a combination thereof, but may consult the Contractor at time of issuance of the TA:

(i) Method of Payment for Task Authorization with Firm Lot Price on Completion: For any authorized Task Authorization issued under the Contract that contains a Firm Lot Price 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 requested by the Contracting Authority 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 Lot Price – 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 requested by the Contracting Authority 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 requested have been completed, delivered, and accepted by Canada.

(iii) Method of Payment for Task Authorizations with a Ceiling Price: For any authorized Task Authorization issued under the Contract that contains a Ceiling 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 Ceiling 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 Ceiling 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 Ceiling price, Canada is only required to pay for the time spent performing the work related to that TA.

7.10.7 Method of Payment – DFMS Instance e-Procurement Solution Transition-In

Canada will pay the Contractor upon completion and delivery of the Work in accordance with Annex 3 – Price Schedule and the payment provisions of the Contract if:

a. an accurate and complete invoice and any other documents requested by the Contracting Authority 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.

7.10.8 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.

7.10.9 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 suppliers of Canada – regardless of their location and/or jurisdiction) for any functionalities and services made available by the Work described in the Contract, 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.

7.10.10 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 Level Requirements (SLR) 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 forecasted by Canada 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 SLR 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 Level Requirements for the Fiscal Year but only some of the PIF objectives and performance measurement criteria have been met, the PA may 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. However, should the Contractor not agree with the amount of Canada's PIF payment for a given year, within 15 business days, the Contractor may present its concerns and Canada will consider these concerns and may revise the PIF payment, if appropriate.

(x) Canada is not bound to use any PIF and may choose not to use the PIF in any given year. Canada is also not bound to use the entire amount of any PIF that is set aside for a given year.

7.10.11 Service Level Failure Credits and Earn-Backs

(i) Payment Credits

Credits for Failure to Meet Minimum Service Level: Starting 6 months following the completion of Milestone #4, if the Contractor fails to meet any of the minimum service levels, identified at subsection 6.13 of Annex 1, Statement of Work, at any given time during the remaining Term of the Contract, the Contractor agrees to credit Canada a payment credit of a percentage of the EPS Operational Firm Lot Monthly Price for that month, for each service level that is not met. The percentage of payment credits associated with each failure to meet a service level are detailed in tables entitled "Contractor Service Level Failure Credits" under each service level.

Maximum Payment Credits: The maximum payment credits per month are capped at 15%. However, if payment credits are incurred for 3 consecutive months, the cap for maximum payment credits in the third month will increase from 15% to 30% and will continue to be capped at 30% for each month in the next 12 month period.

Corrective Measures: 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. Within 5 working days from the end of the month in which the maximum payment credit has increased to 30%, the Contractor must deliver an action plan to the Project Authority and the Contracting Authority and must rectify the underlying problem and meet the required Service Levels within the remainder of the calendar month.

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

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

(iv) Canada's Right to Obtain Payment: These payment 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: Nothing in this section 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 requested 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 (measured monthly). If a service level for the relevant service and any others that Canada determines to be associated with that service are met, or exceeded, during each of the six monthly measurement periods following the service level failure (or period otherwise agreed to by Canada), Canada will return all of the payment credit, associated with that service level, incurred by the Contractor.

(viii) Review of Service Levels

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 Canada begins payment of the EPS Operational Firm Lot Monthly Price, Canada and the Contractor must review the service levels, and may agree to adjustments to them or new requirements as appropriate.

7.11 Invoicing Instructions

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

b. The Contractor's invoice must include a separate line item for each service in compliance with 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.

7.12 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 Term 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.

7.13 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 Term 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.

7.14 Applicable Laws

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

7.15 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. K3030C (2010-01-11), License to Material Subject to Copyright.
c. the general conditions
    i. 2035 (2016-04-04), General Conditions - Higher Complexity - Services
d. Annex 1 – Statement of Work;
e. Annex 2 – Security and Privacy;
f. Annex 3 – Price Schedule;
g. Annex 4 – Security Requirements Check List and Security Classification Guide;
h. Annex 5 – Glossary;
i. Annex 6 – Acronyms;
j. Annex 7 – Task Authorization Form; and
k. 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; and

ii. The Contractor's bid clarification during the bid evaluation process dated _____ (insert date if bid clarification, as required, in any resulting contract).

7.16 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)

7.17 Insurance Requirements

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

SACC Manual clauses G1005C (2016-01-28)

7.18 Limitation of Liability

7.18.1 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. Section 7.18 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 section 7.18 and in any section of the Contract pre-establishing any liquidated damages. The Contractor is liable for indirect, special or consequential damages to the extent described in section 7.18, even if it has been made aware of the potential for those damages.

7.18.2 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 0.25 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.

7.18.3 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 subsection 7.18.3.

7.19 Ownership

7.19.1 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.

7.19.2 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, during the entire Term of the Contract. 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.

7.20 EPS Documentation

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

7.20.2 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.

7.20.3 At no additional cost to Canada, the Contractor must update the EPS Documentation throughout the Term 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.

7.21 Service Rights

7.21.1 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.

7.21.2 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. Neither Canada nor a User will 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.

7.22 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;

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 to Canada.

7.23 EPS Warranty and Maintenance

7.23.1 EPS Warranty:

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

7.24 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 performing the Work, including a license to collect, process, store, generate, and display Canada's Data only to the extent necessary in the provision of the Work.

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 performing the Work, 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.

7.25 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. be responsible for recreating lost Data in the manner and on the schedule set by Canada without charge to Canada; and
e. 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.

7.26 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.

7.27 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 Term of the Contract 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.

7.28 Dispute Resolution

7.28.1 Interpretation

a. "dispute" means any disagreement regarding any issue identified by the Contractor in the notice submitted to Canada in accordance with paragraph 7.28.3.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 paragraph 7.28.1.a.

7.28.2 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.

7.28.3 Notice of Dispute

a. Subject to paragraph 7.28.1.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 will be deemed to have accepted the decision or direction of Canada referred to in paragraph 7.28.3.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 subsection 7.28.4. Negotiation. Such notice must refer specifically to 7.28.4. 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 paragraph 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.

7.28.4 Negotiation

a. Within 10 working days after receipt by Canada of a notice referred to in section 7.28.3. 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 subsection 7.28.4. paragraph 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 may 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, unless Canada and the Contractor agree otherwise.

7.28.5 Mediation

a. If mediation is requested in accordance with subsection 7.28.4. Negotiation, mediation must be conducted in accordance with subsection 7.28.8. Rules for Mediation of Disputes.

b. If a Mediator has not previously been appointed for the purposes of the Contract, a Mediator must be appointed in accordance with subsection 7.28.8. Rules for Mediation of Disputes, forthwith after delivery of a notice in accordance with subsection 7.28.4. Negotiation, requesting mediation.

c. If the dispute has not been resolved within
   i. 30 working days following the appointment of a Mediator in accordance with 7.28.5.b., if a Mediator was not previously appointed;
   ii. 30 working days following receipt by Canada of a responding party's written notice referred to in 7.28.3., "Notice of Dispute", if a Mediator was previously appointed; or
   iii. such other longer period as may have been agreed to by the parties;

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

7.28.6 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.

7.28.7 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.

7.28.8 Rules for Mediation of Disputes

7.28.8.1 Appointment of Mediator

a. The parties to the Contract may, by mutual consent, at any time after entry into the Contract, appoint a 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 Mediator.

b. If the parties do not appoint a Mediator pursuant to subsection 7.28.8.1 paragraph a., the parties must appoint a 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 Mediator must meet the requirements as set out for the contract described in paragraph a. of subsection 7.28.8.1.

c. When mediation is requested pursuant to subsection 7.28.8.1 paragraph a., the parties must within 15 days send to the Mediator
   i. a copy of the notice requesting negotiation under subsection 7.28.3. 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 subsection 7.28.4. Negotiation.

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

e. If the parties have not previously entered into a contract with a mutually acceptable 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 subsection 7.28.9. 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 Mediator, the parties must repeat the process with the Contractor's second selected mediator.

f. Upon execution of the contract with the Mediator the parties must provide the Mediator with copies of the documents referred to in subsection 7.28.8.1 paragraph c.

7.28.8.2 Confidentiality

a. Subject to subsection 7.28.8.2 paragraph b., and unless otherwise agreed in writing by the parties, the 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 Mediator made in relation to mediation are in the 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.

7.28.8.3 Time and Place of Mediation

The 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. Mediation must take place in the NCR or otherwise agreed upon.

7.28.8.4 Representation

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

b. If the Mediator is a lawyer, the 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.

7.28.8.5 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 Mediator must be free to meet with the parties individually during a mediation conference if the 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 Mediator must record that agreement in writing.

7.28.8.6 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.

7.28.8.7 Termination of Mediation

a. Either party may withdraw from mediation at any time without reason and, in that event, the 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 Mediator, either party fails to mediate in good faith or fails to comply with the terms of these Rules, or if the Mediator, at any time during mediation, is of the opinion that further mediation will fail to resolve the issues outstanding, the Mediator may terminate mediation by providing the parties with a written notice of termination, stating therein the 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 Mediator must terminate the mediation by giving written notice to the parties stating the effective date of termination.

7.28.8.8 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 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.

7.28.8.9 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 parties other than Canada and the Contractor, 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 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 Mediator must not be subpoenaed to give evidence relating to
   i. the 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.

7.28.9 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.

7.29 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 paragraph (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.

ANNEX 1

STATEMENT OF WORK

TABLE OF CONTENTS

PART 1: CANADA'S E-PROCUREMENT SOLUTION OVERVIEW

1.1 REQUIREMENT

The Contractor must deliver, enable, implement, support, and manage a bilingual (in English and French) Government of Canada (GC) wide Software as a Service (SaaS) e-Procurement Solution (herein referred to as EPS or the solution) that works, is complete, and provides the functionality to manage the Government of Canada's end-to-end procurement processes.

The Contractor must configure the EPS to ensure compliance with the legislative, regulatory and policy requirements of the Government of Canada and must integrate EPS with the GC's technical environment, including, but not limited to, Departmental Financial and Materiel Management Systems (DFMS). In configuring the EPS, the Contractor must leverage and advise Canada on industry best practices to ensure the EPS supports modern comptrollership and leverages modern procurement, contracting, and financial management best practices.

The EPS provided to the GC by the Contractor must use applications running on a cloud infrastructure. It is not required that the functionality be provided natively within one application, however the Contractor must ensure the applications are integrated into one service offering. The applications must be accessible from various client devices through a web browser. The Contractor must manage and control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, and provide Canada with the capability to configure settings of user-specific applications.

In addition to delivering, configuring, implementing, integrating, and managing the EPS, the Contractor will be required to establish and maintain a service desk and provide services in the application of project, transformation and change management methodologies, tools and processes, including necessary training and communications with Stakeholders and Users.

1.2 SCOPE OF THE WORK

1.2.1 Background

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 procurement opportunities.

The GC is one of the largest public buyers of goods and services in Canada, purchasing approximately $15 billion worth every year on behalf of Federal Departments and Agencies. As the government's main buyer of goods and services (including construction), Public Works and Government Services Canada (PWGSC) is responsible for providing a broad range of procurement solutions to support the delivery of government programs and services. Under this responsibility, PWGSC is acquiring, on behalf of the GC, an EPS to modernize public procurement practices so that they are simpler, less administratively burdensome and deploy modern comptrollership. In order to achieve this objective, the EPS must:

a) Achieve better value for Canadians through improved procurement outcomes;
b) Improve client service by providing easy, web-based access to procurement information and services to Departments and Agencies;
c) Provide easy, web-based access to information and services that reduce Supplier's burden of participating in the procurement process;
d) Achieve an integrated approach to the management of government spend; and
e) Enable procurement professionals with new tools, technology and processes to deliver effective client services.

1.2.2 Scope

The EPS will be used by the GC to manage the Government's procurement process from the point of process initiation (normally associated with needs identification) through the strategic sourcing and procurement lifecycle to close of the Contract.

This procurement may establish a government wide standard for procurement.

The EPS will be used by PWGSC to provide procurement services (source-to-contract) to the GC, while interfacing and operating with clients, Suppliers, and their systems. Procurement professionals within PWGSC will serve as the common services procurement provider for the GC, processing Client initiated requisitions, Sourcing Events, establishing and managing contracts, and establishing and maintaining strategic procurement instruments such as catalogues and associated methods of supply.

GC Users will use the EPS to identify the availability of particular goods and services to meet their requirements, to select item(s) and place Orders directly through e-Catalogues (procure-to-Order), or to initiate a Sourcing Event via a Requisition.

Suppliers to the GC will interact with the GC through EPS for all interactions across the procurement lifecycle - to respond electronically to requests and Orders for goods and services (via the e-Catalogue), to respond electronically or manually to Sourcing Events (RFx), to update their e-Catalogue offerings and to maintain their Supplier profile and information.

Once EPS is operational, other government Departments and Agencies within the GC may, either at their discretion or because the use of EPS for OGDs is made mandatory, begin using EPS to manage contracts and sourcing events within their own departmental delegations.

1.2.3 Solution Vision and Deployment Approach

The EPS is intended to be a government-wide solution for procurement and must be designed, configured, and implemented in consideration of such future scope. However, to manage risks associated with large government IT projects, Canada will proceed with a progressive and gated approach to the broader deployment of EPS, based on successive deployments and successful realization of desired objectives on a limited scale before proceeding to a larger user base.

The first gate of this approach includes the delivery of:

- plans and the solution environment, as articulated in Milestones #1 and #2; and
- a working baseline solution implemented (Milestone #7) with the Acquisitions Program (Acquisitions Branch and the 5 PWGSC Regional offices) of PWGSC and the Finance and Administration Branch (FAB) of PWGSC, as articulated in Milestones #3, #4, #5 and #6.

Following the delivery of Milestone #7, Canada will evaluate if the EPS is meeting the desired objectives and report the results to senior government officials. If Canada determines that the solution should be expanded, Canada may exercise the options in Part 7 – Optional Services to deploy the EPS to a broader user base. Canada anticipates that should the EPS demonstrate success in achieving the desired objectives within the branches of PWGSC, Canada may complete the deployment to the remainder of PWGSC and may invoke the option to deploy up to two additional instances (in addition to PWGSC), as articulated in the Basis of Payment.

If the EPS continues to demonstrate success within the context of PWGSC and additional instances, Canada may seek internal approval to mandate the adoption of the EPS government wide and to establish the EPS as the government wide standard for procurement. If approval is granted, Canada may exercise contractual options to deploy the EPS to rest of the Government of Canada, on a per instance basis, for the remaining DFMS instances. It is anticipated that the deployment to the broader GC may occur over a 2-3 year period, once the options begin to be exercised.

1.2.4 Federated Procurement Model

The EPS must support the GC's federated model for procurement, in which a central organization (Treasury Board Secretariat) sets overarching policies, a common service provider (PWGSC) is responsible for providing a broad range of procurement solutions and services, and government Departments and Agencies have the flexibility (within the regulatory and policy frameworks) to adapt their own procurement operating procedures, processes, forms and approaches to meet their unique operational circumstances. Generally, each Department and Agency has an independent financial management system (or Enterprise Resource Planning System), chart of account, general ledger structure, and approval hierarchy.

PWGSC's procurement services for goods are mandatory for most Departments and Agencies above certain thresholds (generally $25K) while departments may procure services under their own authorities up to certain thresholds (generally $2M). However, PWGSC establishes Methods of Supply which allow Clients to acquire higher values of goods and services when utilizing those instruments. In addition, some Departments and Agencies such as Canada Revenue Agency (CRA) have specific 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 [SSC] for software and hardware for workplace technology devices).

Additionally, the use of PSPC Methods of Supply by most federal government Departments and Agencies are mandatory for 10 commodities (identified below and subject to change from time to time). With the exception of commodities within the mandate of SSC, the catalogues and Suppliers associated with these commodities will be priority areas for onboarding onto the EPS:

1. Information Processing and Related Telecom Services
2. Professional, Administrative and Management Support Services
3. Ground Effect Vehicles, Motor Vehicles, Trailers, and Cycles
4. Telecommunications Equipment and Accessories
5. General Purpose Automatic Data Processing Equipment (including Firmware), Software, Supplies and Support Equipment
6. Furniture
7. Office Machines, text processing systems and visible recording equipment
8. Office Supplies and Devices
9. Clothing, Accessories and Insignia
10. Fuels, Lubricants, Oils and Waxes

1.2.5 Core Functionalities/Uses

The EPS must provide functionalities to support a number of business areas and core procurement functions, including but not limited to the following:

e-Cataloguing (Procure to Order) – the EPS must 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 Users to determine whether required item(s) are available for selection, and to initiate and complete Orders from the applicable e-Catalogue (including Ordering with the use of acquisitions cards). This functionality must 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 with Suppliers which inform each e-Catalogue's structure and contents.

e-Sourcing / CLM (Source to Contract) – when the goods or services required by a User 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 competition is required among the pre-qualified Suppliers to provide the good and/or service, the EPS must provide an e-Sourcing functionality, as described in *Section 3.4 – Sourcing and Contract Management* of this SOW, for GC Users to initiate a Sourcing Event (RFx) to seek bids/arrangements/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. The EPS must provide the functionalities that 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 a one-off-contract.

The full functional scope of requirements that the Contractor must provide is outlined in *Part 3: Functional Requirements* and cover the domains of:

a. General
b. Portal
c. Sourcing and Contract Management
d. Procurement Management

e. Service Procurement Management
f. Financial Management
g. Business Intelligence
h. Supplier Relationship Management
i. Data and Information Management
j. User Management

1.2.6 Government Electronic Tendering Service (GETS)

The Government Electronic Tendering Service (GETS) is the official site for Canada to meet its trade agreement obligations to posts tender notices and allow Suppliers to search for bid opportunities on-line and is the authoritative source for GC tenders. The EPS must provide a new GETS as described in *Section 3.3. Government Electronic Tendering Services* of this SOW that must replace Buyandsell.gc.ca/tenders as the official GETS for the GC.

Within 5 years of ratification of the Comprehensive Economic Trade Agreement (CETA) with the European Union (expected late 2016), the scope of tender notices that are required to be posted on GETS will be expanded to include all Federal Departments and Agencies, and Broader Public Sector tenders covered by the CETA agreement (A list of covered entities is found in Annex X-01 of the CETA agreement).

1.2.7 Canadian Broader Public Sector

On February 26th 2015, the powers of PWGSC were expanded such that it may deliver functions relating to the acquisition, planning and organizing of the provision of goods and services for or on behalf of the government of any province or municipality in Canada, any Canadian aid agency or public health organization or any intergovernmental organization or foreign government. The Canadian Broader Public Sector (BPS) may use EPS to purchase off the GC's e-catalogues on an opt-in basis.

Additionally, GC has included a contractual option that would allow the BPS to acquire the EPS on an opt-in basis at a negotiated price. The BPS would be responsible for the configuration, implementation and funding of their own instances. It is not envisioned that this option would result in a single EPS (or single instance) serving both federal and Broader Public Sector Users. This additional scope will be managed entirely between the service provider and the participating jurisdiction.

1.2.8 Open Data

Canadians require visibility into where their taxpayers' dollars are spent and the GC is committed to providing access to a broad range of open contracting information and data from across Federal Departments and Agencies. The EPS must support GC's Open Data initiative by aggregating and providing procurement data sets contained within EPS for purposes of publishing to Open.canada.ca as Open Data in order to provide Canadians with up to date information regarding procurement activities.

1.3 VOLUMETRIC DATA

Due to the reporting limitations of the legacy systems currently in place, the volumetric data in this Statement of Work is based on limited statistical information and are provided for information purposes only. The data is not to be considered as a contractual guarantee.

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

b) **Contracts and Amendments:** The following table provides a summary of the GC's procurement business volume and value. The table further highlights the activities where PWGSC is providing procurement services to the GC and where departments and agencies are conducting procurements within their own authorities.

Table 1 - GC Business Volume and Value

		PWGSC-AB Procurement Activity 3 years Average (FY12/13 – FY14/15)		GC Procurement Activity (excluding PWGSC-AB) 3 Year Average (CY2011 – CY2013)		Total GC Procurement Activity	
Type of Transaction		**Number of Transactions**	**Value**	**Number of Transactions**	**Value**	**Number of Transactions**	**Value (in $ billions)**
Commodity Management	SA	998	* Value Excluded *	N/A		998	* Value Excluded *
	SA Amendments	2,425				2,425	
	SO	4,142				4,142	
	SO Amendments	5,281				5,281	
Contract Management	Contract	7,785	$9,05B	239,715	$2,80B	247,500	$11,85B
	Contract Amendments	12,067	$4,96B	32,269	$0,20B	44,336	$5,16B
	Call-Ups	1,727	$0,28B	144,315	$1,95B	146,042	$2,24B
	Call-Up Amendments	1,382	$0.05B	19,643	$0,10B	21,025	$0,15B
Total:		**35,808**	**$14,34B**	**435,941**	**$5,05B**	**471,749**	**$19,39B**

c) **Government of Canada Spend Data**

A summary of procurement expenditure data at the Government of Canada level is available at the following link http://open.canada.ca/data/en/dataset/078af0f7-4b15-455d-a466-db5c44409205?_ga=1.13648894.856237901.1448383155.

d) **Government of Canada Spend Data by Department and Agencies**
A summary of procurement expenditure data by Department and Agencies is available at the following link http://open.canada.ca/data/en/dataset/c37d7510-c54c-4652-8e6f-79023e44be62**.**

e) **Population of the Federal Public Service:** The size of each Department and Agency in the federal public service is described at the following link: http://www.tbs-sct.gc.ca/psm-fpfm/modernizing-modernisation/stats/ssa-pop-eng.asp.

Historical information regarding the population of the Federal Public Service is also available as an open data set at the following link: http://open.canada.ca/data/en/dataset/933f8f6e-daee-4368-a7dc-4eadc8b5ecfa

f) **Framework Agreements:** PWGSC manages approximately 2,000 Framework Agreements. As many of these Framework Agreements result in multi-Supplier awards, there are approximately 10,000 supply arrangements and standing offers.

g) **User Base within the GC:** There are approximately 3,100 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 and Agencies (35%). In addition, there are currently over 60,000 users providing administrative services within the GC who 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.

h) **Document, Templates and Forms:** Currently, there are over 200 separate documents, templates and forms used in GC's procurement processes.

i) **Supplier Base:** PWGSC maintains 183,000 Supplier records in its existing Supplier registration database.

j) **Population of Purchasing Group Employees:** Employees within the purchasing group (PG) classification within the GC are the primary federal employees responsible for sourcing and contracting activities in the GC. A breakdown of the current population of PG employees is provided in the table below. It must be noted that sourcing and contracting activities may be performed by employees in other classifications and this list is not inclusive of all potential users of the sourcing and contracting functionality in EPS.

Department	Current Count of Purchasing Group Employees
Administrative Tribunals Support Service of Canada	4
Agriculture and Agri-Food Canada	64
Atlantic Canada Opportunities Agency	8
Canada Border Services Agency	42
Canada Economic Development for Quebec Regions	2
Canada School of Public Service	13

Canadian Grain Commission	6
Canadian Human Rights Commission	2
Canadian Radio-television and Telecommunications Commission	1
Canadian Space Agency	8
Canadian Transportation Agency	1
Canadian Heritage	13
Correctional Services Canada	58
Courts Administration Service	4
Department of National Defence	790
Elections Canada	10
Employment and Social Development Canada	32
Environment and Climate Change Canada	49
Federal Economic Development Agency for Southern Ontario	1
Finance Canada	8
Fisheries and Oceans Canada	86
Global Affairs Canada	108
Health Canada	46
Immigration and Refugee Board of Canada	2
Immigration, Refugees and Citizenship Canada	32
Indigenous and Northern Affairs Canada	28
Infrastructure Canada	3
Innovation, Science and Economic Development Canada	37
Justice Canada	30
Library and Archives Canada	6
Natural Resources Canada	30
Office of the Commissioner of Official Languages	2
Office of the Information Commissioner of Canada	1
Office of the Secretary to the Governor General	5
Parole Board of Canada	1
Privy Council Office	11
Public Health Agency of Canada	7
Public Prosecution Service of Canada	5
Public Safety Canada	5
Public Service Commission	4
Public Works and Government Services Canada	1295
Registrar of the Supreme Court of Canada	2
Royal Canadian Mounted Police	81
Shared Services Canada	99
Statistics Canada	18
Transport Canada	30
Treasury Board of Canada Secretariat	19
Veterans Affairs Canada	12
Western Economic Diversification Canada	1
Total	3122

k) **Departmental Financial Management System (DFMS) Instances:** DFMS instances are installations of particular configurations and applications that form a given Departmental Financial Management System (DFMS) on a given server, supporting a given department or set of departments. The below table describes the GC's DFMS Instances, the software platform, and the departments supported by the given instance.

Software Platform	DFMS Instance	Participating Departments per specific DFMS Instance
SAP R3	Agriculture and Agri-Food Canada	Agriculture and Agri-Food Canada Canadian Pari-Mutual Agency Canadian Food Inspection Agency Canadian Dairy Commission Natural Resources Canada Environment Canada
	Canadian Border Services Agency	Canadian Border Services Agency
	Canadian Heritage	Canadian Heritage Parks Canada
	Canada Revenue Agency	Canada Revenue Agency Canada Revenue Agency - Revenue Ledger
	Canadian Space Agency	Canadian Space Agency
	Immigration, Refugees and Citizenship Canada	Immigration, Refugees and Citizenship Canada Passport Canada
	Global Affairs Canada	Global Affairs Canada Canadian International Trade Tribunal Export Development Corporation
	Employment and Social Development Canada	Employment and Social Development Canada
	Health Canada	Health Canada Hazardous Material Information Review Commission Patented Medicine Prices Review Board Assisted Human Reproductive Agency of Canada Public Health Agency of Canada Indigenous and Northern Affairs Canada
	Innovation, Science and Economic Development Canada	Innovation, Science and Economic Development Canada Canadian Intellectual Property Office of Infrastructure Canada Copyright Board
	Department of Justice	Department of Justice Public Prosecution Service of Canada
	National Research Council	National Research Council
	Department of National Defence	Department of National Defence
	Public Works and Government Services Canada	Public Works and Government Services Canada Shared Services Canada

	Royal Canadian Mounted Police	Royal Canadian Mounted Police Public Safety & Emergency Preparedness Canada
	Treasury Board Secretariat	Treasury Board Secretariat Finance Canada Public Appointments Commission Secretariat Privy Council Office Security Intelligence Review Committee Canada School of Public Service Canadian Transport Agency Office Superintendent Financial Institutions Canada
Oracle	Fisheries and Oceans Canada	Fisheries and Oceans Canada
	Correctional Services Canada	Correctional Services Canada
	Transport Canada	Transport Canada
SAP S4/Hana	GC Financial Management (GCFM)	Atlantic Canada Opportunities Agency Canadian Human Rights Commission Canadian Intergovernmental Conference Secretariat Canadian Transportation Accident Investigation and Safety Board (o/a Transportation Safety Board of Canada) International Joint Commission Office of the Auditor General of Canada Office of the Commissioner of Lobbying Office of the Information Commission Office of the Privacy Commission Office of the Public Sector Integrity Commissioner* Western Economic Diversification Canadian Institutes of Health Research Canadian Nuclear Safety Commission Canadian Radio-television and Telecommunications Commission Courts Administration Service Economic Development Agency of Canada for the Regions of Quebec Financial Transactions and Reports Analysis Centre of Canada Library and Archives Canada Library of Parliament Public Service Commission National Energy Board

		Natural Science and Engineering Research Council Office of the Commissioner for Federal Judicial Affairs Office of the Chief Electoral Officer Office of the Conflict of Interest and Ethics Commissioner Office of the Co-ordinator - Status of Women Parole Board of Canada Office of the Governor General's Secretary PPP Canada (Public Infrastructure, Public Transit, Public Private Partnership) Registrar of the Supreme Court of Canada Senate Ethics Officer The Senate Veterans Affairs Canada Canadian Centre for Occupational Health and Safety Canadian High Arctic Research Station Military Grievances External Review Committee Military Police Complaints Commission of Canada Office of the Communications Security Establishment Commissioner Office of the Commissioner of Official Languages The National Battlefield Commission Statistics Canada

1.4 COMMON TERMINOLOGY

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

PART 2: LEGISLATIVE, REGULATORY AND POLICY REQUIREMENTS

2.1 INTRODUCTION

The EPS must enable GC's compliance with all its acts, regulations, guidelines and policies, as detailed below. All acts, regulations, guidelines and policies are subject to change and the EPS must enable GC's continued compliance with all legislative, regulatory and policy requirements.

Public procurement activities conducted by the 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). The EPS 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.

Where possible, the requirements outlined in *Part 3: Functional Requirements* and *Part 4: Technical Requirements* are structured to allow the GC to comply with the relevant or applicable legislation, regulations, policy, directives, standards and guidelines.

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

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

2.2 ACTS AND REGULATIONS

Access to Information Act
(http://laws-lois.justice.gc.ca/eng/acts/A-1/index.html)
The Privacy Act
(http://laws-lois.justice.gc.ca/fra/lois/P-21/index.html)
Personal Information Protection and Electronic Documents Act (PIPEDA)
(http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html)
Library and Archives of Canada Act
(http://laws-lois.justice.gc.ca/eng/acts/L-7.7/index.html)
Official Languages Act
(http://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html)
Canadian Payments Act
(http://laws-lois.justice.gc.ca/eng/acts/C-21/page-1.html)
Electronic Payments Regulations
(http://laws-lois.justice.gc.ca/eng/regulations/SOR-98-129/)
Secure Electronic Signature Regulations
(http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/)

2.3 POLICIES, DIRECTIVES STANDARDS AND GUIDELINES

Policy Framework for Information and Technology
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12452)
Policy on Information Management
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742)
Policy on Management of Information Technology
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755)
Operational Security Standard: Management of Information Technology Security (MITS)
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328)
Policy on Privacy Protection
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510)
Policy on Access to Information
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453)
Directive on the Administration of the Access to Information Act
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310)
Policy on Government Security
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)
Operational Security Standard on Physical Security
(https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329)
Policy on Financial Management Governance
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14005)
Directive on Electronic Authentication and Authorization of Financial Transactions
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25427)
Policy on Internal Audit
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484)
Policy on *Communications* and Federal Identity
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30683
Directive on Identity Management
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577)
Guideline on Defining Authentication Requirements
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262)
Policy on Acceptable Network and Device Use
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122)

2.4 POLICIES, STANDARDS AND DIRECTIVES GOVERNING ON-LINE SERVICE DELIVERY

Web Standards for the Government of Canada
(https://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/index-eng.asp)
Standard on Web Accessibility
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601)
Standard on Web Usability

(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227)
Standard on Privacy and Web Analytics
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26761)
Standard on Web Interoperability
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25875)
Standard on Email Management
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27600)
Standard on Optimizing Websites and Applications for Mobile Devices
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27088)

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

Financial Administration Act
(http://laws-lois.justice.gc.ca/eng/acts/F-11/index.html)
Comprehensive Land Claim Agreements
(http://www.aadnc-aandc.gc.ca/eng/1100100030577/1100100030578)
Procurement Strategy for Aboriginal Business (PSAB)
(https://www.aadnc-aandc.gc.ca/eng/1100100032802/1100100032803)
Canada's Free Trade Agreements
(http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/fta-ale.aspx?lang=eng)
Agreement on Internal Trade
(http://www.ait-aci.ca/)
Industrial Security
(http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html)
PWGSC Integrity Framework
(http://www.tpsgc-pwgsc.gc.ca/ci-if/ci-if-eng.html)
Data Standard on Classification of Procurement Items
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28305)
Directive on the Application of the Goods and Services Tax/Harmonized Sales Tax
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18930)
Directive on the Payment, Collection and Remittance of Provincial Taxes and Fees
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18929)
Directive on Privacy Requests and Correction of Personal Information
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18311)
Directive on Privacy Practices
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309)
National Joint Council Travel Directive
(http://www.njc-cnm.gc.ca/directive/index.php?did=10&dlabel=travel-voyage&lang=eng&merge=2&slabel=index)
Security and Contracting Management Standard
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12332)

PWGSC Supply Manual
(https://buyandsell.gc.ca/policy-and-guidelines/Supply-Manual)
Standard on Vendor Record
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25845)
Procurement Strategy for Aboriginal Business: Guidelines for Buyers/Government Officials (http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/contpolnotices/97-6-eng.asp)
Retention Guidelines for Common Administrative Records of the Government of Canada (http://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/retention-common-administrative-records/Pages/introduction.aspx)
Sources of Federal Government and Employee Information 2009, Index of Standard Personal Information Banks
(http://www.infosource.gc.ca/emp/emp04-eng.asp)
Canadian International Trade Tribunal Act.
(http://laws-lois.justice.gc.ca/eng/acts/c-18.3/)
Policy on Green Procurement
(http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html)
Procurement Review Policy
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12074)
Canadian Content Policy
(https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/annex/3/6)
Contracting Policy
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14494)
Policy on Title to Intellectual Property Arising Under Crown Procurement Contracts
(http://www.ic.gc.ca/eic/site/068.nsf/eng/00005.html)
Policy Notices and TB Circulars - Contracting
(http://www.tbs-sct.gc.ca/hgw-cgf/business-affaire/gcp-agc/notices-avis/index-eng.asp)
Contracting Policy Notice 2007-04 - Non-Competitive Contracting (http://www.tbs-sct.gc.ca/hgw-cgf/business-affaire/gcp-agc/notices-avis/2007/0920-eng.asp)
Common Services Policy
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12025)
Employment Equity Policy
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12543)
Government Contracts Regulations
(http://laws-lois.justice.gc.ca/eng/regulations/SOR-87-402/FullText.html)
Procurement Ombudsman Regulations
(http://laws-lois.justice.gc.ca/eng/regulations/SOR-2008-143/index.html)
Department Public Works and Government Services Act
(http://laws-lois.justice.gc.ca/eng/acts/P-38.2/index.html)
Standard on Enterprise Resource Planning Systems
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25687&section=text)
Policy on the Stewardship of Financial Management Systems
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=17589)

Directive on Stewardship of Financial Management Systems
(http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=17590)

2.6 IT SECURITY GUIDELINES

IT Security Guidance
(https://www.cse-cst.gc.ca/en/group-groupe/its-advice-and-guidance)
ITSG-41 Security Requirements for Wireless Local Area Networks
(https://www.cse-cst.gc.ca/en/node/264/html/15287)
ITSG-33 IT Security Risk Management: A Lifecycle Approach
(https://www.cse-cst.gc.ca/en/node/265/html/22814)
ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones
(https://www.cse-cst.gc.ca/en/node/266/html/25034)
ITSG-31 User Authentication Guidance for IT Systems
(https://www.cse-cst.gc.ca/en/node/267/html/22784)
ITSG-04 Threat and Risk Assessment Working Guide has been replaced by the Harmonized Threat And Risk Assessment Methodology (TRA)
(https://www.cse-cst.gc.ca/en/publication/tra-1)
ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada
(https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg22-eng_0.pdf)
IBISI
(http://iss-ssi.pwgsc-tpsgc.gc.ca/gvrnmnt/risi-iisr-eng.html)

PART 3: FUNCTIONAL REQUIREMENTS

3.1 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. The Contractor must perform the following activities and provide an EPS that provides the following, but not limited to, functionalities:

a) be an easy to use and a flexible tool that can be readily configured by Users to reflect their specific requirements.
b) Allow defined User roles and responsibilities based access to the EPS and its functionalities.
c) have workflow and business rules (including audit and compliance capabilities) to be configured by Users to support a wide variety of processes, activities and functions (as further described below).
d) 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.
e) 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.
f) allow for seamless data sharing within the solution and to and 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.
g) allow for dynamic and Near Real-Time access to data, reporting and analytic information to support the effective management of the GC, monitoring and tracking of procurement processes and performance, and management and business decision-making.
h) allow Suppliers to securely create and manage their own User accounts through credential based access to the EPS.

The Contractor must fully integrate all functional requirements described in sections A to J of *Part 3: Functional Requirements* of the SOW.

Note to Bidders: If a Bidder is awarded points for indicating that its EPS will provide functionalities in response to evaluation criterion *R6. Additional Functional Requirements* of *Attachment 2 to Part 4 – Technical Evaluation* and that Bidder is awarded a Contract, the Bidder will be contractually obliged to provide all the functionality it identified as being provided with its EPS. The GC will incorporate these functionalities in the following corresponding section (sections A to J).

3.2 SECTION A – GENERAL REQUIREMENTS

The General Requirements section identify high level functions and outcomes that are applicable across all elements of the EPS.

Table 2 - General Requirements

SOW NUM	Requirement
A-01.00	Deleted
	Deleted
A-02.00	**Search** The Contractor must deliver a solution that provides the functionality to:
A-02.01	Search based on reportable fields, document attributes and Metadata i. Deleted ii. Deleted iii. Deleted iv. Deleted v. Deleted vi. Deleted vii. Deleted viii. Deleted ix. Deleted x. Deleted
A-03.00	**Usability & User Interface** The Contractor must deliver a solution that provides the functionality that:
A-03.01	i. Deleted ii. Deleted iii. Deleted iv. Deleted v. Deleted vi. Deleted vii. Deleted viii. Deleted ix. For Authorized Administrators to configure existing business artifacts and attributes, create new artifacts and attributes and control business behaviour (such as conditions that must be met before user can amend an order) using business rules. Specifically, they must be able to a) add new attributes or modify functionality of existing attributes, b) Set attribute type (number, free text, money, pick list, Boolean, uploaded attachment/document, look up, etc.) c) Set attribute GUI position and tab order d) Set attribute level behaviour and properties (labels, mouse over help, mandatory/optional, visibility, default value, etc.)

SOW NUM	Requirement
	e) Create business and validation rules f) Set print layout g) Specify which attributes are internal to EPS and which ones will be shared with the supplier (in RFX, Order, etc.) h) Specify which data attributes are pre-populated when the artifact is created (such as prepopulate user data from the requester's user profile on a requisition when a requisition is created) i) Specify which data attributes are carried forward to related business artifacts in a process (example – creating orders from shopping carts) j) Specify which attributes are included when the Business artifact is copied. k) Specify the behaviour (business rules, validation rules, etc.) that apply when the business artifact is modified.
A-03.02	to track and display changes (history) for each business artifact (requisitions, orders, etc.). Changes include modifications to information, workflow approval/denial, submissions to vendors, and confirmations from vendors.
A-04.00	**Online Help** The Contractor must deliver a solution that provides the functionality to:
A-04.01	i. Provide a configurable Reference section that contains links to quick reference guides, manuals and policies; ii. Provide in-application help and User support for functionality and processes; iii. Deleted iv. Deleted and v. Enable presentation of context sensitive help topics aligned with the section of the EPS the User is currently on.
A-05.00	**Error Messages & Notifications** The Contractor must deliver a solution that provides the functionality to:
A-05.01	i. Allow Authorized Administrators to configure and control system notifications and notification triggers; ii. Deleted .
A-06.00	**Documentation** The Contractor must:
A-06.01	i. Provide the Government of Canada (GC) all documentation and collateral material that is available for its current commercial offering and all future releases; ii. Deleted iii. Deleted iv. Deleted

SOW NUM	Requirement
A-07.00	**Electronic Authorizations and Secure Electronic Signatures** The Contractor must deliver a solution that provides the functionality:
A-07.01	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: i. Access to electronic systems that store or process financial or finance-related transactions is restricted to those who require it to perform their duties; ii. User authentication information, such as identifiers and passwords, are properly safeguarded and managed, and Users understand their accountabilities; iii. 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; iv. The Users approving transactions, including those exercising account verification, monitor the accuracy and appropriateness of the transactions and are informed of their accountabilities; v. 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 vi. An audit trail is maintained and records retention and disposition are managed in 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 Authorized Administrators to create and configure web based forms
A-08.02	for Authorized Administrators to: i. Set fields as mandatory or optional; ii. Configure and set default values for common data entry fields; iii. Add user-defined fields to any screen in various transactions; iv. 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; v. Configure and create different types of extrinsic fields (e.g. text, radio groups, checkboxes, drop-down lists, money, date, etc.); and vi. Modify out of the box field labels.
A-08.03	to automatically notify Users of incomplete mandatory data fields.
A-08.04	Deleted

SOW NUM	Requirement
A-08.05	Interoperability with SAP DFMS: i. Ensure all relevant purchasing, financial and workflow approval information is communicated between both systems; ii. Ensure near real time verification of budget availability in the DFMS; iii. Have the ability to route transactions from EPS to the proper delegated authority for approval within the DFMS; and iv. Reconcile all Procure to Pay (P2P) information including receipt of goods/services and payment information between EPS and DFMS.
A-09.00	Deleted
A-09.01	Deleted

3.2.1 Workflow

The EPS must 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 3 - General Requirements – Workflow

SOW NUM	Requirement
A-10.00	**Workflow - General** The Contractor must deliver a solution that provides the functionality:
A-10.01	for Authorized Administrator to create, configure and manage automated workflow approval process templates for each business artifact (such as requisitions, RFXs, supplier profile, user profile, etc.). Authorized Administrators must be able to configure workflow approval process templates based on system data, business rules, and groups/roles/permissions. For each workflow stop, the Authorized Administrators must be able to configure a) the sequence (position of this stop versus other stops), b) whether it is sequential or parallel, c) who it is assigned to (group or individual), d) the action required (watcher only, approve/deny or edit/approve/deny) e) list of acceptable reasons for approving or denying f) escalation rules (length of time dormant, group or individual to escalate to)
A-10.02	Deleted
A-10.03	Deleted

SOW NUM	Requirement
A-10.04	for users 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	Deleted
A-10.06	Deleted
A-10.07	for Users to provide a reason and comments when approving/denying
A-10.08	Deleted
A-10.09	for users to view the status of the item in workflow
A-10.10	Deleted
A-10.11	Deleted
A-10.12	Deleted
A-10.13	Deleted
A-10.14	Deleted
A-10.15	to enable the use of a graphical or textual tool for creating and configuring workflows and testing
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.

3.2.2 Workload

The EPS must provide GC Users with the ability to assign files and activities to other GC Users, to monitor and measure performance against assigned tasks, as well as to effectively allocate and re-allocate workload across multiple Users, User groups and organizations.

Table 4 - 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 Authorized Administrators to configure and manage lists of procurement team Users (e.g. by division, category and commodity taxonomy).
A-11.02	for Authorized Users to configure business rules for automatic assignment of groups or individual members of a procurement team.
A-11.03	for Authorized Users to manage team members participating in the sourcing event.
A-11.04	Deleted
A-11.05	Deleted

SOW NUM	Requirement
A-11.06	Deleted
A-11.07	Deleted
A-11.08	Deleted
A-11.09	Deleted
A-11.10	Deleted
A-12.00	**Workload - Tracking and Status** The Contractor must deliver a solution that provides the functionality:
A-12.01	to track and record performance metrics on business artifacts (e.g. created date, submitted date, approved date, etc.)
A-12.02	Deleted
A-12.03	Deleted
A-12.04	to track and link requisition with all components of procurement file.

3.2.3 Taxes

A-13.00	**Taxes** The Contractor must deliver a solution that provides the functionality to:
A-13.01	to calculate the taxes in accordance with Canadian tax laws.
A-13.02	to calculate the taxes on the requisition and shopping cart requests.

3.3 SECTION B – PORTAL REQUIREMENTS

3.3.1 Objective

The EPS must service a large, complex organization where Users come from various external Suppliers and internal departments and agencies, each with multiple levels of hierarchy and have varying delegations on a commodity specific and general basis. The Contractor must provide access to the Portal functionalities specified below and outlined within the various sections of the Statement of Work in order to establish a secure, reliable and accessible environment for all Users:

a) **Bilingual Interface:** the EPS must deliver a comprehensive bilingual interface to all Users (internal and external) to the solution and associated services, information, training and support and present all Users with at-a-glance information that is most relevant to their roles and responsibilities;

b) **Content and Data:** the EPS must allow Users to create, edit, review, approve and publish content in the Portal.

c) **Landing Page:** the EPS must allow for the creation and configuration of specific page(s) on a web site for the general public including:

i. Registration to generate a User profile;
ii. Deliver relevant communications;
iii. Provide information on what is available through the EPS; and
iv. enable one-time login for Users and have authenticated access to all components of the EPS;

d) **Dashboards:** the EPS must have a dashboard with the following functionalities:

i. Set goals and expectations for specific individual Users or groups;
ii. Encourage specific actions in a timely manner;
iii. Highlight exceptions and provide alerts when problems occur;
iv. Communicate progress and success; and
v. Provide a common interface for interacting with and analyzing important business data.

e) **Communication:** the EPS must enable and facilitate the delivery of key messages to Users.

3.3.2 Government Electronic Tendering Services (GETS)

The Contractor must provide the functionality to deliver, enable and support a tendering Portal as described in this section.

3.3.2.1 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 GC's Government Electronic Tendering Service (GETS) must be provided as a part of the EPS. The GETS platform does not need to be in the same solution environment as long as it delivers, enables and supports the functional and technical requirements described in this SOW.

Procurement policies require the GC 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 service known as BuyandSell.gc.ca/tenders since 2013. EPS will replace the BuyandSell.gc.ca/tenders GETS platform.

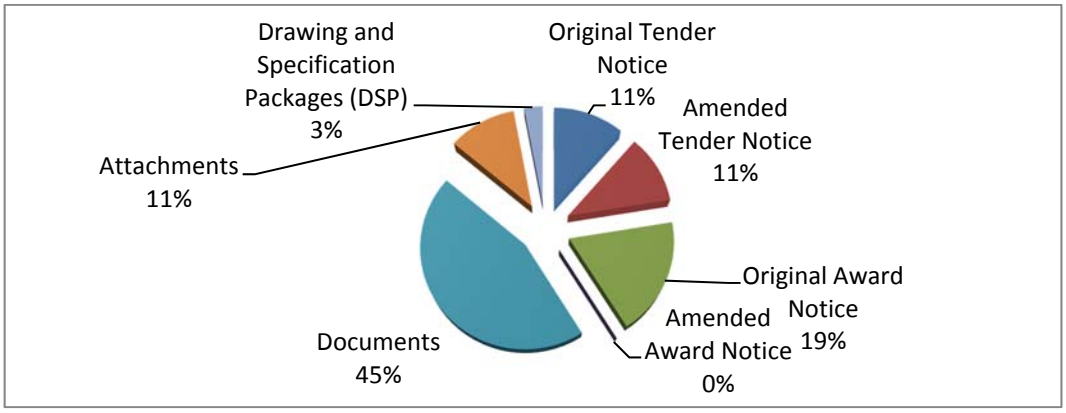
3.3.2.2 Public Tender Volumetrics:

Over a 12 month 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).

Figure 1 - Buyandsell.gc.ca – Metrics



3.3.2.3 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. The EPS must provide the functionalities to allow Authorized Users to post such notices and other procurement related notices.

3.3.2.4 Comprehensive Economic Trade Agreement (CETA)

To meet the requirements of CETA with the European Union, the GC must provide a GETS on which all Canadian public sector tender notices subject to this trade agreement must be published. This capability will be required within 5 years of the ratification of the CETA which is targeted for late-2016.

All GC tender notices must be posted in both official languages.

As the single point of access for government tenders, EPS must deliver, enable and support multiple sources and methods for creating tender notices, including:

a) The creation and publication of tender notices including attachments through EPS as part of an e-sourcing activity.
b) The manual creation and publication of tender notices including attachments without creating a sourcing event in EPS.
c) The aggregation, publication, and updating of tender notices including attachments from third party systems and data feeds.
d) The configuration of publishing cycle times for batch or individual transmission of tender notices.
e) Automatic update of active tender notice (including attachments) in support of any revisions initiated and approved through EPS (e.g. amendments, cancellation, and termination).
f) 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).

g) Automatic application and control of tender notice status and version (e.g. Active, Amended #, Expired, Cancelled, and Awarded).
h) Automatic archiving of expired procurement opportunities so they are separate from open bid opportunities.

3.3.2.5 Contract Award Notices

For procurements subject to trade agreements, a Contract Award Notice must be posted through EPS 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 Exception" to posting requirements has been invoked. For procurements subject to the trade agreements where EPS is not used for contract award, the EPS must provide the functionality to manually create and post award notices.

3.3.2.6 Services Supporting Supplier Access to Opportunities

The ability for Suppliers to easily find and access government opportunities is paramount. EPS 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's EPS must provide Users the functionality to:

a) 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 the tenders.

b) Subscribe and receive web feeds for specific bid opportunities they intend on responding to in EPS.

c) Search published tender notices, save, bookmark and share the URL (the Webpage address) without requiring Users to be logged in. The URL must stay the same when new information becomes available.

d) Organize, filter and sort all open bid opportunities; and access tender notices by goods and services categories (e.g. 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).

3.3.2.7 Services Supporting Supplier Ability to Analyse Opportunities and Forge Partnerships

The Contractor must provide the functionality for Suppliers to analyse published opportunities and identified potential partnerships. It must also provide functionalities to deliver, enable and support the following objectives:

a) List of Interested Suppliers (Bidder Request List): 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.

b) Deleted

c) 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.

3.3.2.8 Open Tender Data

The 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 individuals to participate in government through information sharing. The GC is committed to ensuring data on government opportunities is freely available. All procurement data on GETS from the EPS must be provided in Open Data format for easy download by any individual.

GETS must be an open service which 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 *Part 3 Section I Data and Information Management*. The Contractor must not restrict the ability for third parties to re-publish tender information.

3.3.3 Portal Requirements

Table 5 - Portal Requirements

SOW NUM	Requirement
B-01.00	**General** The Contractor must deliver a solution that provides the functionality:
B-01.01	for Authorized Users to electronically and in Near Real-Time create, edit, view, and publish content in the Portal.
B-01.02	for Users to view current and expired system notices in the Portal.
B-01.03	Deleted
B-02.00	**Login 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 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:

SOW NUM	Requirement
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	Deleted
B-03.03	Deleted
B-03.04	Deleted
B-03.05	Deleted
B-03.06	for Users to organize their dashboard
B-03.07	Deleted
B-03.08	Deleted
B-03.09	Deleted
B-03.10	Deleted
B-03.11	Deleted
B-03.12	Deleted
B-03.13	Deleted
B-03.14	Deleted
B-03.15	for Users to view, search and organize (e.g. sort and filter) their work activities
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 GC
B-04.02	for Users to access all electronic communications within EPS between GC Users 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/goods receipt, credit memo).
B-04.04	to notify Users when Supplier has acknowledged their requests (e.g. request for quote), Orders and messages within EPS;
B-04.05	for Authorized Administrators to create and distribute electronic, outward communication to Portal Users.
B-04.06	to communicate to all Users or a subset of Users (e.g. at a minimum, being able to create e-mail distribution lists).
B-04.07	Deleted
B-04.08	Deleted

SOW NUM	Requirement
B-05.00	**Government Electronic Tendering Service (GETS)** The Contractor must deliver a solution that provides the functionality:
B-05.01	Deleted
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	Deleted
B-05.04	for Authorized Users to manually create and publish tender notices including attachments to GETS
B-05.05	to automatically update active tender notices (including attachments) on GETS in support of any revisions initiated and approved through EPS (e.g. amendments, cancellation, termination).
B-05.06	Deleted
B-05.07	to automatically archive expired tender notices so they are separate from open bid opportunities.
B-05.08	Deleted

3.4 SECTION C - SOURCING AND CONTRACT MANAGEMENT

3.4.1 Objective

The Contractor and its EPS must provide a Consumer-Like experience guiding the User through the requisition creation process, and provide online collaboration between Users during all phases of a sourcing event.

Where an item is not located within an existing e-Catalogue, the EPS must provide the functionality for Users to submit a Requisition to initiate a Sourcing Event. The initiation of a Requisition must trigger, within the EPS, the development of the procurement plan and strategy, where decisions will be made that will contribute to the development of an RFx. The EPS must then provide the functionality to develop an RFx to solicit offers/proposals from one or more Suppliers.

The EPS must provide the functionality for Users with administrative rights to establish templates for RFx, which will provide for configurable and customizable electronic documents that will then be populated, in the EPS, by other GC Users based on the confirmed procurement plan and strategy and the specifics of the GC User's requirements for goods and/or services. The EPS must provide the functionality for the GC User to 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. The Contractor must ensure that the applicable information persists from the Sourcing Event to the e-Catalogue area without requiring the information to be extracted from the EPS, manipulated and then imported to the e-Catalogue. The EPS must provide the functionality to

distribute the resulting RFx document (which includes the Catalogue Data File) directly to one or more Supplier(s) or to be publicly posted for access by any potential Supplier(s).

The e-Sourcing functionality of the EPS must 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 must provide a secure means of Supplier bid creation and submission (for electronic proposals) and recording of bid receipt (for hard-copy proposals).

The EPS must provide the functionality to include, in the RFx, 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 Users may collaborate with other 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 Authorized Users to create and award a contract/Framework Agreement; including the necessary reviews and approvals.

The EPS must provide the functionality, when creating a Sourcing Event, for the User to configure the RFx 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 the award of a contract, 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 deliver functionality for Users to conduct 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 and/or services Ordered by the GC User 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 Users) where appropriate.

The EPS functionalities must be fully configurable to effectively manage sourcing events and contracts in compliance with all government objectives, policies, rules and regulations.

The EPS will be used to conduct one-off / complex procurement processes; to establish new or refresh existing Framework Agreements/Methods of Supply; to create or maintain e-Catalogues and for Ordering e-Catalogue items where a second-stage procurement process is required.

This Sourcing and Contract Management section is divided into the following sub-sections:

C-01 Requisition Management - the EPS must enable a User to create, edit, save and electronically submit requisitions to authorize a GC User 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 Deleted

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 Suppliers to securely submit electronic bids and paper-based bids.

C-06 Evaluation - the EPS must provide the functionalities to enable Authorized Users to evaluate 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 or Agency 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 Authorized 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 Administrators to create and manage a clause repository (library) providing corporate and custom clauses in both official languages that can be accessed by Authorized Users to create RFx, RFx amendments, contracts, and contract amendments.

3.4.2 Requirements

Table 6 - 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, configure and manage requisitions
C-01.02	Deleted

SOW NUM	Requirement
C-01.03	Deleted
C-01.04	to assign a unique identifier to create a linkage between all relevant documents (e.g. contract, requisition and solicitation).
C-01.05	Deleted
C-01.06	to update requisition status through its lifecycle (e.g. Draft, Submitted for Approval, Amended, Rejected).
C-01.07	Deleted
C-01.08	for GC Users to: i. Create, view, save, retrieve, modify and amend Requisition with a minimum of 9,999 line items; and ii. Link supporting documents to the Requisition.
C-01.09	Deleted
C-01.10	for GCs User to electronically certify availability of funds
C-01.11	for GC Users to assign multiple financial codes to a Requisition line item.
C-01.12	Deleted
C-01.13	Deleted
C-01.14	for Authorized Users to manually enter requisitions and requisition amendments into EPS.
C-01.15	To track requisitions throughout the procurement process
C-02.00	Deleted
C-02.01	Deleted
C-02.02	Deleted
C-02.03	Deleted
C-03.00	**RFx Creation** The Contractor must deliver a solution that provides the functionality:
C-03.01	for Authorized Users to create and manage single and multi-phase Sourcing Events (e.g. LOI, RFI, RFP linked to single Requisition).
C-03.02	Deleted
C-03.03	for Authorized Users to search central repositories for various artefacts and templates during RFx creation including,

SOW NUM	Requirement
	i. Deleted ii. Deleted iii. Deleted iv. Deleted v. Deleted vi. Deleted vii. Deleted
C-03.04	Deleted
C-03.05	for Authorized Users to search, identify, reference and/or import applicable clauses and conditions
C-03.06	Deleted
C-03.07	Deleted
C-03.08	Deleted
C-03.09	Deleted
C-03.10	Deleted
C-03.11	to support of “sealed bidding” process.
C-03.12	Deleted
C-03.13	Deleted
C-03.14	for Authorized Users 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 models including, but not limited to, open competitive, invitational competitive and directed procurement process.
C-04.02	for Authorized Users to create and manage reusable source lists
C-04.03	Deleted
C-04.04	Deleted
C-04.05	for Authorized Users to manage bidding period and amend closing date

SOW NUM	Requirement
C-04.06	Deleted
C-04.07	for Authorized Users to send electronic notification(s) to all or selected Suppliers from a source list. (ex. informing them of the procurement opportunities, changes to the solicitation)
C-04.08	for Authorized Users to modify published solicitations and for EPS to send an electronic notification to Suppliers when a solicitation they are participating in is modified.
C-04.09	to support Near Real-Time and scheduled posting on GETS of Sourcing Events, notices and associated documents.
C-04.10	for Authorized Users to cancel an existing solicitation and publish a cancellation notice to the GETS.
C-04.11	Deleted
C-04.12	Deleted
C-04.13	for Suppliers to electronically submit questions on the solicitation.
C-04.14	for Authorized Users to edit Supplier questions before: i. Deleted ii. Sharing and/or publishing questions and answers with all participating Suppliers at the same time iii. Deleted
C-04.15	Deleted
C-04.16	for Authorized Users to generate reports or view information regarding supplier activity on an RFx that, at minimum, details the number of Suppliers who viewed and downloaded the RFx.
C-05.00	**Bid Submission** The Contractor must deliver a solution that provides the functionality:
C-05.01	for Suppliers to complete and submit electronic bids
C-05.02	to store and secure electronic bids access to submitted bids until the designated bid closing time.
C-05.03	to disable electronic bid submission functionality at bid closing time.
C-05.04	to allow Authorized user to manually enter bid submissions received outside EPS and set the submitted date and time of each submission. i. Deleted ii. Deleted iii. Deleted iv. Deleted v. Deleted

SOW NUM	Requirement
	vi. Deleted
C-05.05	To generate an official record (electronic receipt) for both on-line and off-line bid submissions
C-05.06	for Suppliers to retract submitted bids and resubmit final bid prior to bid closing time.
C-05.07	Deleted
C-05.08	Deleted
C-05.09	Deleted
C-06.00	**Bid Evaluation** The Contractor must deliver a solution that provides the functionality:
C-06.01	to keep bid evaluation information accessible only to Users that are a part of the evaluation.
C-06.02	for Authorized Users to access bid submissions after bid closing.
C-06.03	for Authorized Users to provide Users with access to technical bids for evaluation purposes.
C-06.04	for Users to document their evaluation results using pre-configured evaluation grids with embedded formulas.
C-06.05	Deleted
C-06.06	Deleted
C-06.07	to enable and support individual and consensus team evaluation processes
C-06.08	for the evaluator to save the bid evaluation results and continue work later before submitting final result of evaluation.
C-06.09	Deleted
C-06.10	to capture technical/financial evaluations and scoring based on criteria established in the sourcing process.
C-06.11	to calculate the final bid score based on RFx defined formulas and selection methodology.
C-06.12	Deleted
C-06.13	Deleted
C-06.14	Deleted
C-07.00	**Contract Award** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
C-07.01	To ensure all mandatory requirements configured in EPS are met before awarding contract.
C-07.02	for Authorized Users to award contracts
C-07.03	Deleted
C-07.04	for Authorized Users to create new contract by copying information from an existing contract template.
C-07.05	for Authorized Users to add a minimum of 9,999 line items to the contract.
C-07.06	Deleted
C-07.07	for Authorized Users 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 Authorized Users to create contracts that include one or more pricing features (as selected by the User) including, but not limited to, firm 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 Authorized Users 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 Authorized Users to create and award contracts, agreements and contractual documents
C-07.11	for Authorized Users to create and award one contract against multiple requisitions.
C-07.12	for Authorized Users to award one or multiple contracts, Framework Agreements from a single solicitation
C-07.13	for Authorized Users to create, award and manage contract and contract related documents electronically.
C-07.14	for Authorized Users to award a contract to a Supplier by applying preconfigured business rules, formulas and algorithms from a Sourcing Event.
C-07.15	to publish and persist line item level contracts to the EPS catalogue
C-07.16	for Authorized Users to delay, suppress or retract posting of Contract Award Notice and provide justification.
C-07.17	for Authorized Users to configure and publish Contract Award Notice on GETS once a contract is awarded and signed.
C-07.18	Deleted
C-07.19	for Authorized Users to modify contract elements (e.g. financial coding, contracting authority) through an automated approval workflow process.
C-07.20	Deleted

SOW NUM	Requirement
C-08.00	**Contract Administration** The Contractor must deliver a solution that provides the functionality:
C-08.01	Deleted
C-08.02	Deleted
C-08.03	for Authorized Users to track, monitor, validate and manage contractual work progress and performance of the Supplier.
C-08.04	for Authorized Users to configure triggers to facilitate the tracking and management of contractual events such as, but not limited to, deliverable and milestone due dates, validity period, renewal dates, Supplier reporting obligations, usage of funds, effort, under the contract.
C-08.05	for Authorized Users to manage contract amendment requests and all resulting changes to the contract.
C-08.06	for Authorized Users to create, approve, manage and control contract amendments.
C-08.07	for Authorized Users to activate, manage, and remove contract suspension including the resumption of work once the suspension has been lifted.
C-08.08	for Authorized Users to terminate a contract and update the status of published contract award notice on GETS.
C-08.09	Deleted
C-08.10	Deleted
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 Authorized Users to create and manage procurement files by linking together all documents related to a sourcing event including, but not limited to: i. Assignment of common unique identifier for linking requisition, contract and all associated procurement file documents; ii. Link all information related to the solicitation process and contract creation (e.g. evidence of approvals, risk assessments, procurement planning documents, requisition and any amendments); iii. Link all information related to the bid evaluation process (e.g. bid evaluation plan, resulting evaluation documents); iv. Link records of actions taken during a contract lifecycle (e.g. correspondence, records of phone discussions, formal records of meetings, meeting minutes, records of decisions); v. 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.

SOW NUM	Requirement
C-09.02	Deleted
C-09.03	Deleted
C-09.04	Deleted
C-09.05	Deleted
C-09.06	Deleted
C-09.07	Deleted
C-09.08	Deleted
C-09.09	Deleted
C-09.10	Deleted
C-10.00	**Central Repository** The Contractor must deliver a solution that provides the functionality:
C-10.01	for Authorized Administrators to create and manage a clause repository (library) in both official languages that can be accessed by Authorized User to create RFx, RFx amendments, Contracts, and contract amendments.
C-10.02	for Authorized Administrators to identify corporate and custom clauses and designate clauses that require a workflow to be modified.
C-10.03	for the system to 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	Deleted
C-10.06	Deleted
C-10.07	Deleted
C-10.08	Deleted
C-10.09	Deleted
C-10.10	Deleted
C-10.11	Deleted

3.5 SECTION D - PROCUREMENT MANAGEMENT

3.5.1 Objectives of Procurement Management

The Contractor and its EPS must provide functionalities, within the e-Catalogue environment, to:

a) Provide a Consumer-Like experience to guide the User through the Ordering Process, while ensuring that the eventual Order is in full compliance with the Framework Agreement
b) Reduce the risk of the User Ordering the incorrect product or service
c) Provide a 'one stop' online store for Users to search electronic catalogues and view approved goods and services though a Framework Agreement established by the GC
d) Apply and enforce business and financial rules and approvals to Orders
e) Ensure compliance to terms and conditions of Framework Agreements
f) Electronically submit Shopping Cart requests and Orders to Suppliers from EPS
g) Facilitate flow of transactional communication between the Supplier and the GC
h) Maintain an audit trail of all transactions
i) Provide full reporting and monitoring functionalities

3.5.2 Background Information on Framework Agreements

The GC has a number of existing Framework Agreements (also known as Methods of Supply) that it has established; particularly for the procurement of Mandatory Standing Offers and Supply Arrangements (https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/3/5/1) which will continue to maintain and may be updated over time. The GC will continue to establish new Framework Agreements as needs arise based on its continued strategic review of procurement requirements, spend analysis and historical trends.

Only PWGSC can establish Framework Agreements that can be used by other Departments and Agencies, as well as the Canadian Broader Public Sector. Any Department or Agency can establish a Framework Agreement for their own use with the exception of those covered by 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
- Audio Visual Equipment
- Clothing & Textile
- Commercial Training
- Communication Services
- Engineering 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.

3.5.2.1 Framework Agreement Types

Depending upon the overarching Framework Agreement(s) an e-Catalogue may take one of the following forms:

a) **Simple e-Catalogue(s)** – which must allow GC Users to browse, select and request goods and/or services that are defined.

b) **Configurable e-Catalogue(s)** – which must allow GC Users to browse, select and request goods and/or services where the GC User can select from among available options to configure (e.g. color, accessories, hard drive size, warranty) the goods (e.g. Vehicles, Computers) and services (e.g. Professional Services) that they are requesting.

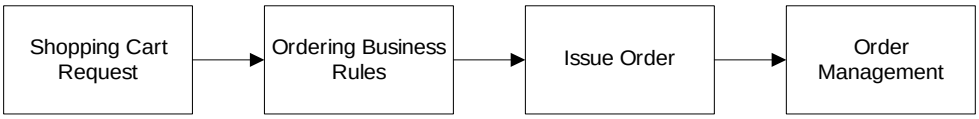
c) **Complex e-Catalogue(s)** – which must allow GC Users to browse, select and request more complex goods and/or services. In a complex catalogue, the GC User will need to develop and send to the pre-qualified Supplier(s) a Statement of Work (SOW), to which the pre-qualified Supplier(s) will be required to respond before an Order may be placed.

d) **Two-Stage Selection Process** – For requirements that require a second-stage selection process (using the Supply Arrangement), a RFx process will be initiated based on the applicable business rules using the Sourcing and Contract Management functionalities of the EPS.

3.5.2.2 Ordering Process

The EPS must enable the following Ordering Process. When a need is identified, a User must be able to easily navigate and to search the e-Catalogue to determine if there is a Framework Agreement with the good(s) and/or service(s) they are seeking.

Where an item is available, a GC User may then select the items and add them to a Shopping Cart, when the User submits their Shopping Cart, through the applicable 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.) will then be triggered and a Shopping Cart request is sent to the applicable Supplier(s) 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. If a Catalogue does not allow a Supplier to reject a Shopping Cart request and there are no Ordering business rules then instead of a Shopping Cart request being sent to a Supplier, it would be sent as an Order.



The Procurement Management functionalities 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 (on time, on budget, right quality, etc.); to amend Orders (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.

3.5.3 Ordering Business Rules

The EPS must provide the functionality to configure the Ordering business rules that must ensure openness, fairness, transparency and integrity of the Ordering process for multi-Supplier sourced Methods of Supply. The Ordering business rules must provide the built-in controls to respect the Terms & Conditions of the Method of Supply to ensure that the Orders are issued in an objective manner which meets the following socio-economic objectives of the GC;

a) Reducing barriers to small and medium enterprise business by providing them an equal opportunity to compete with larger firms;
b) Respecting all legislation, regulations, policy;
c) Ensuring a fair distribution of Orders amongst the qualified Suppliers for the applicable Method of Supply for the selected goods and services;
d) Provides best value to the GC;
e) Enhancing the integrity and efficiency of the acquisition process.

3.5.4 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 EPS must provide the functionalities to accommodate the GC's Supplier Selection Methodologies. These methodologies include configuring: 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.

3.5.5 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 procurement obligations associated with Comprehensive Land Claims Agreements. 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 Authorized User will create a Catalogue Data File using the applicable catalogue attributes (e.g. Part #, Item Description, Price). Once the structure is created, the Authorized User will then populate the Catalogue 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 Authorized User 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 EPS, 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 Authorized User 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 must 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 an Authorized Administrator.

3.5.6 Requirements

Table 7 – 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 catalogues including the functionality to i. add new fields and set field type (number, free text, pick list, Boolean, uploaded attachment/document, etc.) ii. set business and validation rules iii. Set field level behaviour (labels, mouse over help, mandatory/optional, visibility, default value, etc.) iv. Specify which fields are internal to EPS and which ones will be shared with the supplier (on requisitions and orders.) v. Specify which data attributes are pre-populated when the catalogue or catalogue line item is created vi. Specify which fields are copied to the shopping cart when a line item is added to the shopping cart
D-01.02	Deleted
D-01.03	for Users to view the history for their shopping carts and Orders.
D-01.04	Deleted
D-01.05	for Users to be able to search for their Shopping Cart requests and Orders.
D-01.06	for Authorized Administrators to configure Shopping Cart requests and Orders.
D-01.07	Deleted
D-01.08	for Users to execute a 'Quick Quote' with selected Suppliers for non-catalogue purchases under an identified dollar threshold or commodity where more than one Supplier exists prior to submitting it for approval and eventual Purchase Order.
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 (e.g. product numbers, pictures and descriptions) in a Catalogue Data File.

SOW NUM	Requirement
D-02.02	for Catalogue content to be displayed in the preferred language of the User.
D-02.03	for Authorized Users and Suppliers to manage access to view and purchase from PunchOut catalogues
D-02.04	to export Catalogues into different Catalogue Data File formats in order to allow an Authorized User to work off-line in the Catalogue Data File and to import it back into EPS.
D-02.05	Deleted
D-03.00	**Catalogue - Creation** The Contractor must deliver a solution that provides the functionality:
D-03.01	for Authorized Users to create simple, configurable, and complex 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	For Authorized Users to create the configuration options (e.g. hard drive size for a computer) for a configurable Catalogue item (e.g. Computers, Vehicles) to be selected by the User in the Shopping Cart.

SOW NUM	Requirement
D-03.03	for Authorized Users to manage Method of Supply attributes (e.g. Authorized Users, 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) for an individual Catalogue and to apply them during the Ordering Process. for Authorized Users to configure view and order privileges for catalogues (may be based on MOS, contract, catalogue, commodity, organization, user, region, role, etc.) for Authorized Users to create and manage shopping cart and ordering business rules such as minimum and maximum order thresholds (may be based on MOS, contract, catalogue, commodity, organization, user, region, role, etc.) for Authorized Users to be able to specify supplier limitations for the MOS, Contract or Catalogue that prevent users from submitting shopping cart requests or placing orders once the cap has been reached. for Authorized Users to be able to specify the MOS, Contract or Catalogue limitations (e.g. dollar value cap or % of total amount cap) that prevent users from submitting shopping cart requests or placing orders once the limitation has been reached. For Authorized users to set and manage additional MOS, Contract, Catalogue or Commodity information (such as terms and conditions, comprehensive land claims agreements, set aside for aboriginal business) that will be used by business rules on the catalogue, shopping cart, catalogue requisition and order.
D-03.04	Deleted
D-03.05	Deleted
D-03.06	Deleted
D-03.07	Deleted
D-03.08	Deleted
D-03.09	Deleted
D-03.10	Deleted
D-03.11	Deleted
D-03.12	for Authorized Administrators to configure what fields and attributes are displayed in a Shopping Cart request (e.g. Supplier part number, description, Unit of Measure, unit price, calculated total price, need-by-date, payment & shipping terms) associated to the applicable Catalogue in order to ensure only the relevant fields and attributes are displayed to the User.
D-03.13	Deleted

SOW NUM	Requirement
D-03.14	for Authorized Users 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	Deleted
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	Deleted
D-04.03	Deleted
D-04.04	Deleted
D-05.00	**Catalogue - Catalogue Data File** The Contractor must deliver a solution that provides the functionality:
D-05.01	Deleted
D-05.02	Deleted
D-05.03	for Authorized Users to configure minimum shopping cart values, for goods and services in a given MOS, Commodity or Catalogue,
D-05.04	Deleted
D-05.05	Deleted
D-05.06	Deleted
D-06.00	**Catalogue - Pricing** The Contractor must deliver a solution that provides the functionality:
D-06.01	Deleted
D-06.02	to identify the currency (e.g. USD, CDN, EUR) of the pricing attribute(s) of a Catalogue File.
D-06.03	To support regional catalogues, including the functionality: i. For Authorized Users to be able to specify if a MOS is national or regional. ii. For Authorized Users to be able to map regional MOS to one or more regions. iii. To be able to map users to one or more regions. iv. To be able to indicate the region on the shopping cart. v. To restrict users to only view and order from national MOS or their regional MOS catalogues. vi. To set pricing using MOS, Catalogue and region.
D-06.04	Deleted
D-06.05	for Authorized Users to configure and manage tiered pricing for items on each Catalogue that are used to determine pricing on an individual shopping cart.
D-06.06	Deleted
D-06.07	for Authorized Users and Suppliers to manage and update the price list information for Catalogues
D-07.00	**Catalogue - Management** The Contractor must deliver a solution that provides the functionality:

SOW NUM	Requirement
D-07.01	for Authorized Users to examine, manage, verify and approve catalogue content within the solution.
D-07.02	for Authorized Users to browse, search, sort, and filter any field within a Catalogue.
D-07.03	for version control of a Catalogues and to record and display the version number, uploaded/modified date, approved date and published date
D-07.04	for Authorized Users to view all versions of the catalogue.
D-07.05	for Authorized Users to compare the new and previous Catalogue versions and determine changes made.
D-07.06	Deleted
D-07.07	for Authorized Users to add/remove/update any Catalogue line item.
D-07.08	for Suppliers to submit updated Catalogue Data Files for review and approval.
D-07.09	for Authorized Users to schedule the effective date/time when an initial Catalogue or updated Catalogue is published (both with Method of Supply and individual Catalogue level) for client use.
D-07.10	Deleted
D-07.11	Deleted
D-07.12	Deleted
D-07.13	Deleted
D-07.14	for Authorized Users to activate or deactivate catalogues or catalogue line items.
D-07.15	for Authorized Users to import and upload Catalogue updates on behalf of the Supplier.
D-07.16	for Suppliers to electronically update Catalogue through an automated self-service process standard data upload integration (example through web services or Electronic Data Interchange).
D-07.17	Deleted
D-07.18	for when a Method of Supply end date has passed, to deactivate the related Catalogue File.
D-07.19	Deleted
D-08.00	**Shopping Cart - General** The Contractor must deliver a solution that provides the functionality:
D-08.01	for user to create a Shopping Cart request on behalf of another User and Client.
D-08.02	To assign a unique identifier to each version of a Shopping Cart request and orders. To link shopping carts to related orders.
D-08.03	Deleted
D-08.04	to compare Catalogue items according to their specifications (e.g. price, size, weight, benchmark evaluation).
D-08.05	to capture additional information about an item (e.g. moving to and from, comments, restrictions) to be specified via a web form.
D-08.06	to determine the line item price according to the regional price set in the catalogue and the region specified by the user on shopping cart.
D-08.07	for Users to collaboratively work with Suppliers on defined Shopping Cart items through a configurable form (e.g. for services requirements).

SOW NUM	Requirement
D-08.08	to allow Suppliers to submit the content of their response to a Shopping Cart request until the configurable response deadline.
D-08.09	Deleted
D-08.10	Deleted
D-08.11	Deleted
D-09.00	**Shopping Cart - Search** The Contractor must deliver a solution that provides the functionality:
D-09.01	for Authorized Users 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	Deleted
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	Deleted
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.
D-09.10	Deleted
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 use EPS business rules and other information to determine the final price for each item (discounts, tiered pricing, etc.).
D-10.03	at the header level and/or 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	Deleted
D-10.05	Deleted
D-10.06	for the management of delivery addresses including the functionality i. to default the delivery address from the address in the user's profile ii. for users to change the delivery address by choosing from a master delivery address list iii. for user to manually enter a delivery address iv. for Authorized Administrators to configure workflow to route shopping carts with manually entered delivery address for approval
D-10.07	Deleted

SOW NUM	Requirement
D-10.08	Deleted
D-10.09	Deleted
D-10.10	Deleted
D-10.11	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-10.12	Deleted
D-10.13	to support multiple shipping addresses for items on a shopping cart.
D-10.14	Deleted
D-10.15	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 EPS validates that the product no longer exists so Shopping Carts cannot proceed) when saving the shopping cart, submitting the shopping cart for approval and at final approval (before creating order(s)).
D-10.16	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-10.17	Deleted
D-10.18	to fully support PunchOut catalogues.
D-10.19	to allow users to add items from multiple catalogues to the same shopping cart.
D-10.20	Deleted
D-10.21	to create a Shopping Cart request by executing a search of the Catalogue content and selecting items.
D-10.22	for Users to initiate a non-Catalogue requisition.
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 group together items according to similar product variants.
D-11.03	to include pictures as part of a Catalogue search result.
D-11.04	Deleted
D-11.05	to display the base price of a good or service before additional features are selected.
D-11.06	Deleted
D-12.00	**Shopping Cart - Management** The Contractor must deliver a solution that provides the functionality:
D-12.01	Deleted
D-12.02	Deleted
D-12.03	for Users to change elements in the Shopping Cart (e.g. the quantity of items ordered, delivery date and shipping address) prior to placing the Order.
D-12.04	for Users to update old Shopping Cart requests to generate a new Shopping Cart request.

SOW NUM	Requirement
D-12.05	for Users to save the Shopping Cart for later retrieval.
D-12.06	Deleted
D-13.00	Deleted
D-13.01	Deleted
D-14.00	**Ordering Business Rules- General** The Contractor must deliver a solution that provides the functionality:
D-14.01	Deleted
D-14.02	for Suppliers to withdraw a proposal to a Shopping Cart request up to the time of Order issuance.
D-14.03	Deleted
D-14.04	Deleted
D-14.05	Deleted
D-15.00	Deleted
D-15.01	Deleted
D-15.02	Deleted
D-15.03	Deleted
D-15.04	Deleted
D-15.05	Deleted
D-16.00	**Ordering - General** The Contractor must deliver a solution that provides the functionality:
D-16.01	to display the total Order price taking into account all applicable costs and discounts.
D-16.02	for Users to save, modify or cancel Orders
D-16.03	to notify the User of an Order rejection and a reason why (e.g. insufficient resources to complete the Order, delivery issues).
D-16.04	to restrict visibility and access to existing Orders based on User roles.
D-16.05	to ensure all Orders are tracked against the applicable Method of Supply.
D-16.06	Deleted
D-16.07	Deleted
D-16.08	to issue the Order in the applicable currencies of the Catalogue.
D-17.00	**Ordering - Creation** The Contractor must deliver a solution that provides the functionality:
D-17.01	to use role based security, business rules and system business information to restrict User's ability to issue orders.
D-17.02	Deleted
D-17.03	Deleted
D-17.04	Deleted
D-17.05	Deleted
D-17.06	Deleted

SOW NUM	Requirement
D-17.07	to notify applicable Users and update shopping cart/order status when an Order could not be successfully transmitted
D-17.08	Deleted
D-17.09	Deleted
D-17.10	Deleted
D-17.11	Deleted
D-18.00	**Ordering – Management** The Contractor must deliver a solution that provides the functionality:
D-18.01	for Authorized Administrators to configure the order print layout, and for users to be able to print an Order.
D-18.02	for Users to Change an Order.
D-18.03	for a User to initiate a workflow process based on a Method of Supply and the termination reason through a pre-configured selectable list of reasons (e.g. default, mutual consent, for convenience of the Crown), to terminate an Order along with supporting documentation.
D-18.04	Deleted
D-18.05	Deleted
D-18.06	Deleted
D-18.07	Deleted
D-18.08	Deleted
D-18.09	Deleted
D-19.00	**Ordering - Display** The Contractor must deliver a solution that provides the functionality:
D-19.01	Deleted
D-19.02	for Users to view the Catalogue item associated to any document throughout the Order process.
D-19.03	Deleted
D-19.04	for Users to view and drill down all Shopping Cart requests tied to an Order.
D-19.05	Delete
D-20.00	Deleted
D-20.01	Deleted
D-20.02	Deleted
D-20.03	Deleted
D-20.04	Deleted
D-20.05	Deleted
D-20.06	Deleted
D-21.00	Deleted
D-21.01	Deleted
D-21.02	Deleted
D-21.03	Deleted

SOW NUM	Requirement
D-22.00	Deleted
D-22.01	Deleted
D-22.02	Deleted
D-22.03	Deleted
D-22.04	Deleted
D-22.05	Deleted
D-22.06	Deleted
D-22.07	Deleted
D-22.08	Deleted
D-22.09	Deleted
D-22.10	Deleted
D-22.11	Deleted
D-22.12	Deleted
D-22.13	Deleted
D-23.00	**Card Management** The Contractor must deliver a solution that provides the functionality:
D-23.01	to deliver level 2 enhanced data (such as card holder information, transaction amount, transaction date, currency code and conversion, merchant name, sales tax, customer reference number (EPS order number)) on acquisition card charges.
D-23.02	To support supplier specific ghost cards.
D-23.03	To support user specific acquisition cards.
D-23.04	To send ghost card or acquisition card payment information to the supplier on electronic orders.
D-23.05	To import acquisition card charges into EPS and match them with the appropriate order (for level 2 ghost card charges) or with the user (for user specific acquisition card charges).

3.6 SECTION E - SERVICE PROCUREMENT MANAGEMENT

The Contractor and its EPS must support Service Procurement in terms of e-Sourcing and creation of e-Catalogues.

3.6.1 Catalogue

The objective of the Catalogue sub-section of requirements is to describe the configurability and management of the content in service catalogues specifically, in addition to the requirements outlined in *Section 3.5 - Procurement Management*. It also describes requirements related to the linking of specific resource categories to standardized resource qualifications.

3.6.2 Shopping Cart

The objective of the Shopping Cart sub-section is to describe the requirements that are required for services catalogues, in addition to the requirements outlined in the *Section 3.5 - Procurement Management*.

3.6.3 Ordering

The objective of the Ordering sub-section is to describe the requirements that are required for services catalogues, in addition to the requirements outlined in the *Section 3.5 - Procurement Management*.

3.6.4 Statement of Work (SOW) Management

The objective of this the SOW Management sub-section of requirements is to ensure robust SOW functionalities that must be provided within the EPS, specifically to allow the GC to recall, reuse and amend previous SOWs or create new ones in order to award single or multiple Contracts. The requirements for the Contractor in this section describe the creation of new SOWs in a variety of ways, including manually (either within or outside the EPS), filling out specific fields of a standardized SOW, selecting content from a SOW Builder, and 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. The e-Catalogue functionalities 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.

3.6.5 Resource Management – Performance Management

The objective of the Resource Management – Performance Management sub-section is to describe how Supplier 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.

3.6.6 Master Resource Record

The objective of the Master Resource Record sub-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:

a) To reduce duplication and streamline the process for managing resource data in the EPS; and
b) 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.

3.6.7 Requirements

Table 8 - 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 shopping cart 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 Users 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 Authorized Users to create and manage resource qualification requirements using a combination of mandatory criterion and point rated criteria 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 allow Authorized Users to set fixed prices, ceiling prices, and rates for geographical areas and individual categories and sub-categories for all Suppliers or to set individual prices for individual Suppliers.
E-02.04	Deleted
E-02.05	to allow Authorized Users 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-02.06	Deleted
E-03.00	**Shopping Cart - Proposal Evaluation** The Contractor must deliver a solution that provides the functionality:
E-03.01	Deleted
E-03.02	to notify the Supplier that their proposal contains incomplete fields (e.g. has not responded to each individual qualification and/or has not attached the necessary documentation)
E-03.03	Deleted
E-03.04	Deleted
E-03.05	to complete an offline evaluation and import the evaluation results
E-03.06	Deleted
E-03.07	Deleted
E-03.08	for Users to accept or reject resource proposals including explanatory comments and send the information to the supplier.

SOW NUM	Requirement
E-04.00	**SOW Management General** The Contractor must deliver a solution that provides the functionality:
E-04.01	Deleted
E-05.00	**SOW Management - Manual Creation** The Contractor must deliver a solution that provides the functionality:
E-05.01	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 EPS or importing one that was created outside the EPS.
E-06.00	**SOW Management - Standard SOW Creation** The Contractor must deliver a solution that provides the functionality:
E-06.01	to allow Authorized 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-07.00	Deleted
E-07.01	Deleted
E-07.02	Deleted
E-07.03	Deleted
E-07.04	Deleted
E-07.05	Deleted
E-08.00	**SOW Management - SOW Library** The Contractor must deliver a solution that provides the functionality:
E-08.01	to configure and manage a library of sample SOWs by central and/or Authorized Administrators.
E-08.02	Deleted
E-09.00	**SOW Management - SOW Amendments** The Contractor must deliver a solution that provides the functionality:
E-09.01	for Users to amend an existing SOW at any point during the contract lifecycle (e.g. adding deliverables).
E-09.02	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-10.00	**Ordering - Management** The Contractor must deliver a solution that provides the functionality:
E-10.01	for Users to create and manage Orders with a combination of time and material and deliverable-based services.
E-10.02	Deleted
E-10.03	Deleted
E-10.04	to allow Users to manage and track dates for Orders for services involving multiple deliverables and/or milestones (e.g. date received, comments).
E-10.05	Deleted

SOW NUM	Requirement
E-10.06	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-10.07	Deleted
E-10.08	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-10.09	for Users to configure optional periods, optional work, and optional quantities for their Order.
E-11.00	Deleted
E-11.01	Deleted
E-11.02	Deleted
E-11.03	Deleted
E-11.04	Deleted
E-12.00	**Master Resource Record** The Contractor must deliver a solution that provides the functionality:
E-12.01	to store information in a Master Resource Record that can be accessed by Users at any time.
E-12.02	for Authorized Administrators to create and manage resources using a unique identification, regardless of the Supplier organization.
E-12.03	to store and access 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-12.04	for Authorized Administrators to configure a workflow to validate submitted resource qualifications and certificates prior to User acceptance.
E-12.05	Deleted
E-12.06	Deleted
E-12.07	Deleted
E-12.08	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.

3.7 SECTION F - FINANCIAL MANAGEMENT

Is included as an optional service under section 7.2.6 of this Statement of Work.

3.8 SECTION G - BUSINESS INTELLIGENCE

3.8.1 Overview

Business Intelligence (BI) section of requirements describe functionalities for the Contractor and its EPS to ensure there is a technology-driven process for analyzing data and presenting reportable information to help executives, managers and other Users make more informed business decisions. The BI requirements

encompass a variety of tools, applications and methodologies that enable the GC 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 Intelligence requirements are 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)

3.8.2 Requirements

Table 10 - 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: i. All User entered and defined data fields (e.g. contract fields, attributes, metadata, and geographic areas); ii. All system captured and stored data; iii. All aspects of procurement process (e.g. from Requisition to Payment); and iv. 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 : i. Tabular; ii. Columnar; iii. Cross tab or pivoted; and iv. 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: i. Purchasing orders; ii. Requisitions; iii. Catalogue items; iv. Contracts; v. Sourcing projects; and vi. Suppliers.

SOW NUM	Requirement
G-01.05	Deleted
G-01.06	Deleted
G-01.07	Deleted
G-01.08	Deleted
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: i. MS Excel/MS Word; ii. CSV file; iii. XML file; and
G-01.10	to configure report parameters and performance metrics for reporting on various procurement activities, including, but not limited to: i. Performance trends (e.g. Supplier, quality, time, contract); ii. Contract metrics (e.g. spend %, leakage %); iii. Changes in Contracts and Orders (dollar amount, quantities); iv. Deleted v. Pre-defined or User defined Key Performance Indicators (KPI) thresholds; and vi. 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.
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: i. Requisition related operational reports; ii. Bid evaluation related operational reports; iii. Contract related operational reports; iv. Purchasing Order related report; v. Operational reports that can show various procurement summary information; and vi. Operational reports for all workload activities.
G-02.02	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-02.03	Deleted
G-03.00	**Analytics** The Contractor must deliver a solution that provides the functionality:
G-03.01	Deleted

SOW NUM	Requirement
G-03.02	Deleted
G-03.03	Deleted
G-03.04	to aggregate fact table measurement data by key data elements
G-03.05	Deleted
G-03.06	Deleted
G-03.07	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-03.08	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	Deleted
G-04.01	Deleted

3.9 SECTION H - SUPPLIER RELATIONSHIP MANAGEMENT

3.9.1 Overview

Supplier Relationship Management (SRM) section of requirements describe the functionalities that the Contractor must provide for the management of Supplier registration, and for enabling the capture, tracking and measurement of Supplier performance.

This section provides functionalities for the Contractor to ensure the EPS provides end-to-end Supplier lifecycle supporting capability for the GC to lower costs, reduce risk, and facilitate relationships with Suppliers. The SRM section provides functionalities for 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. Functionalities of the SRM that must be provided by the Contractor include:

a) **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;
b) **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 Supplier performance, financial risk, ecological profile, pending litigation, contracts etc.
c) **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 Supplier corrective action as required.

d) **Supplier performance management 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.

e) **Supplier's self-registration:** EPS must provide functionality to allow the Supplier to self-register and securely manage their own profile online. EPS must also allow for GC stakeholders (e.g. Industry Canada, CRA, PWGSC, INAC) to validate profile information against other GC systems via the Enterprise Service Bus. As part of the self -registration process, Suppliers to the GC must be able to store, in the EPS, corporate information and documents such as, but not limited to, applicable licenses, certifications, insurance certificates and security clearances.

The SRM section is divided into 5 sub-sections:

- **H-1 Supplier Profile Management** (functions to support Supplier self-registration, using predetermined and secured access permissions)
- **H-2 Performance** (functions to assess Suppliers' 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 of the EPS 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.)

3.9.2 Requirements

Table 11 - 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: i. Approvals and tasks when Supplier registers; ii. Recurring tasks; and iii. Variations in registration process (e.g. by commodity, by region, by Supplier status).
H-01.02	Deleted
H-01.03	for Authorized Administrators to configure Supplier profile questions in order to collect Supplier credentials and certification and store them under Supplier's profile at various times, including, but not limited to: i. When Supplier registers into the EPS; and ii. When Supplier completes and submits a response to an RFx.
H-01.04	Deleted
H-01.05	to support parent/child Supplier organizational hierarchies and tree like classification and management of Suppliers.
H-01.06	to support storage, maintenance and retrieval of documents from the Supplier's profile including, but not limited to: i. Credentials; ii. Certifications; iii. Insurance policies; and iv. Financial statements.
H-01.07	to ensure completeness of Supplier's data and data quality including, but not limited to: i . Preventing duplication of Suppliers; and ii. Raising the alerts on Suppliers with missing, incomplete as well as mismatching data in their profile
H-01.08	to utilize a single and unique Supplier ID number across the entire procurement process and allow traceability of a Supplier throughout the process.
H-01.09	to enable Supplier to set up their interests for a single or multiple commodities (e.g. by commodity code, by service offering, by region).
H-01.10	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: i. Import and attach electronics copies of their qualifications certifications in multiple

SOW NUM	Requirement
	formats (e.g., PDF, .PPT, .BMP, .GIF, .JPEG, .JPG); and ii. Enter and update validity period of qualifications and certifications (e.g. expiry dates).
H-01.11	Deleted
H-01.12	to define, associate and maintain Supplier registration with and locational information including, but not limited to: i. deleted ii. geographical zones; and iii. Regions (from Region Master List).
H-01.13	Deleted
H-01.14	Deleted
H-01.15	Deleted
H-01.16	to create and manage supplier registration for joint ventures including i. to allow Supplier to create a unique supplier profile for a joint venture ii. to ensure each member of the joint venture has their own supplier profile iii. to link the joint venture profile to each member's supplier profile iv. to indicate which member (if applicable) will act on behalf of all members v. to automatically input joint venture profile and joint venture member profile information into bid proposals vi. to allow Supplier and Authorized Administrators to add or remove vendors from a joint venture vii. to workflow changes to joint venture profiles to an Authorized User if the joint venture profile is associated with an active MOS
H-02.00	**Performance** The Contractor must deliver a solution that provides the functionality:
H-02.01	for Authorized Users to record and monitor Supplier performance throughout the contract lifecycle.
H-02.02	for Authorized Users to add notes on Supplier performance.
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 Authorized Users to access Supplier performance evaluation history information and data at any time including but not limited to: i. During the RFx evaluation; ii. During Contract Management; and iii. During procurement File Close-Out.
H-02.05	for Authorized Users to create configurable surveys and scorecards to assess and report on Supplier performance including, but not limited to performance on: i. Orders;

SOW NUM	Requirement
	ii. Framework Agreements; iii. Contracts; and iv. Overall performance.
H-02.06	to allow drill-down and roll-up up on Key Performance Indicators to evaluate results on a more detailed level.
H-02.07	for Authorized Administrators to configure and maintain process to debar a Supplier that includes, but is not limited to: i. Configuration of workflow to govern (e.g. set, remove) debarment and handle exceptions; ii. Configuration of alerts and triggers that prompts Users of debarred Suppliers; iii. Configuration of business rules that would prevent a User from issuing contracts, orders, or Framework Agreements to debarred Supplier; iv. Configuration of business rules with decision points that can prevent or allow debarred Suppliers to bid on competitive procurements; and v. Configuration of business rules with a decision points that would make debarred Supplier's catalogues unavailable to Users.
H-02.08	for Authorized Users to debar a Supplier through workflow managed process and business rules including, but not limited to debarment: i. Across-the-board (affecting all aspects of the Supplier's operations); ii. For a specific period of time; iii. For a specific geographic region; iv. For a specific commodity; and v. 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	Deleted
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: i. Any data field within the Supplier repository; ii. Any data field within the survey and scorecard library; and iii. Any data field within the performance evaluations.
H-04.02	for Authorized Administrators to perform faceted searches to find and view Suppliers and Suppliers' information including, but not limited to: i Supplier data; ii. Contract history; iii. Contact information;

SOW NUM	Requirement
	iv. Qualifications; v. Certifications; and vi. 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 track and notify Authorized Users throughout the procurement process when and if, Supplier's performance status is updated and changed within SRM such as, but not limited to: i. Proposed winning Supplier had performance issues on previous and /or current contract(s); ii. Supplier is debarred; and iii. Supplier is suspended.
H-05.02	to allow for mass notification to Suppliers of announcements, changes to ongoing sourcing events or other communications.

3.10 SECTION I - DATA AND INFORMATION MANAGEMENT

3.10.1 Objective

The objective of this section is to describe the requirements for Data and Information Management to be provided by the Contractor within the overall scope of the EPS to ensure that:

a) Information needs are met from different perspectives: GC Procurement policies, processes and regulations; Suppliers' business needs; Users from GC Departments and Agencies; stakeholders and partners.

b) Information reaches high quality standards and retains its business value over its lifetime.

c) Information is seamlessly flowing between various systems and databases.

d) Procurement master data (classifications, Supplier) is constantly evolving through manual and automated processes such as reviews, adjustment and enrichment.

e) Data assets are preserved from system failures and recovery mechanisms are agreed upon, planned and implemented.

f) Public information is available and shared with partners on a continuous basis (e.g. Open Data).

g) 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 EPS must be robust, comprehensive, and based

on commercially available, off-the-shelf data management technologies.

3.10.2 Requirements

Table 12 - 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	Deleted
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.
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	Deleted
I-03.01	Deleted
I-03.02	Deleted
I-03.03	Deleted
I-03.04	Deleted
I-03.05	Deleted
I-03.06	Deleted
I-04.00	**Reference & Master Data Management** The Contractor must deliver a solution that provides the functionality:
I-04.01	Deleted

SOW NUM	Requirement
I-04.02	for Authorized Administrators to create, configure and manage master data such as Material Master Record and Vendor (Supplier) Master Record.
I-04.03	Deleted
I-04.04	Deleted
I-04.05	Deleted
I-04.06	Deleted
I-04.07	Deleted
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: i. Using a blank or pre-defined template; ii. Importing (upload) an existing document; iii. Cloning an existing document as a new one; and iv. Deleted
I-06.03	for Metadata information to be captured during the creation of document
I-06.04	Deleted
I-06.05	for the management of documents (e.g. modify, remove).
I-06.06	Deleted
I-06.07	Deleted
I-06.08	Deleted
I-06.09	Deleted
I-06.10	Deleted
I-06.11	Deleted

SOW NUM	Requirement
I-06.12	Deleted
I-06.13	Deleted
I-06.14	Deleted
I-06.15	Deleted
I-06.16	Deleted
I-06.17	Deleted
I-06.18	Deleted
I-06.19	Deleted
I-06.20	Deleted
I-06.21	Deleted
I-07.00	**Metadata Management and Taxonomy** The Contractor must deliver a solution that provides the functionality:
I-07.01	Deleted
I-07.02	for the import and export of taxonomy structure and terms using standard formats (e.g. CSV, XML).
I-07.03	Deleted
I-07.04	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-07.05	Deleted
I-07.06	Deleted
I-07.07	Deleted
I-07.08	Deleted
I-07.09	Deleted
I-07.10	Deleted
I-07.11	Deleted

3.11 SECTION J - USER MANAGEMENT

3.11.1 Objective

The objective of this section is to describe the requirements for the Contractor to allow the GC to manage Users.

3.11.2 User Management Requirements and Deliverables

This section includes roles/groups requirements, registration requirements, profiles/accounts requirements, and login requirements. The main deliverables include:

3.11.2.1 Roles/Groups

The Contractor must provide the capability to assign groups (likely consisting of types and roles) to Users. This capability must 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 and roles with a variety of access rights and privileges.

3.11.2.2 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.

3.11.2.3 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.

3.11.2.4 Login

The Contractor must provide the functionalities to allow for authentication of the User at login through the use of an electronic credential key.

3.11.3 Requirements

Table 13 - 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).

SOW NUM	Requirement
J-01.05	to allow for a variety of roles for Users with a variety of access rights and privileges (e.g. administrator, auditor, finance, manager, procurement officer, reviewer, trainer, contracting officer, buyer, requisitioner, unspecified User, etc.).
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.
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	Deleted
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	to create and manage configurable User profile information which can be used as attributes within the solution (e.g. consignee code, region, language preference, contact details, manager name, credit card information).
J-03.02	for Authorized Administrators to modify, disable, or close individual User profiles in EPS.
J-03.03	to retain User account records within EPS for access by Authorized Administrators for a defined time period (configurable).
J-03.04	for Authorized Administrators to clone User profiles for use by new Users (authorities, settings, etc.) and modify specific elements of the profiles.
J-03.05	for Authorized Administrators to manage User accounts once they are created (e.g. send notifications to Users related to account use and functionality).
J-03.06	for Authorized Administrators to search, display, and modify changes to the profile of any User.
J-03.07	Deleted
J-03.08	Deleted

SOW NUM	Requirement
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 EPS using an electronic credential key.

PART 4: TECHNICAL REQUIREMENTS

4.1 INFORMATION TECHNOLOGY AND SOLUTION MAINTENANCE AND UPDATES

4.1.1 e-Procurement Solution

The Contractor must deliver, enable, and maintain an EPS including relevant information technology hardware and software components and related business processes to deliver the functional requirements detailed in the SOW. The EPS must 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. The EPS components must have the functionality to interact and integrate with IT components used by GC and delivery partners. The EPS must include management and operations support of the scalable, robust, resilient on-demand computing and network infrastructure.

4.2 HARDWARE REQUIREMENTS

GC is procuring an EPS as a Software as a Service (SaaS). As such, no installation of hardware, other than network connectivity pieces, upon GC premises will be permitted for the purpose of this Contract.

The Contractor must provide, develop, configure, test, maintain and house all infrastructure 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 INTERFACES WITH GOVERNMENT OF CANADA SYSTEMS

4.3.1 Background

In order to develop and support 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 to:

a) 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
b) identify and specify the high level data exchange requirements with other departmental systems and non-GC data sources.

The requirements in *Section 4.4 EPS Technology Requirements* 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). The EPS rollout plan will set the standards and methods for interoperability with

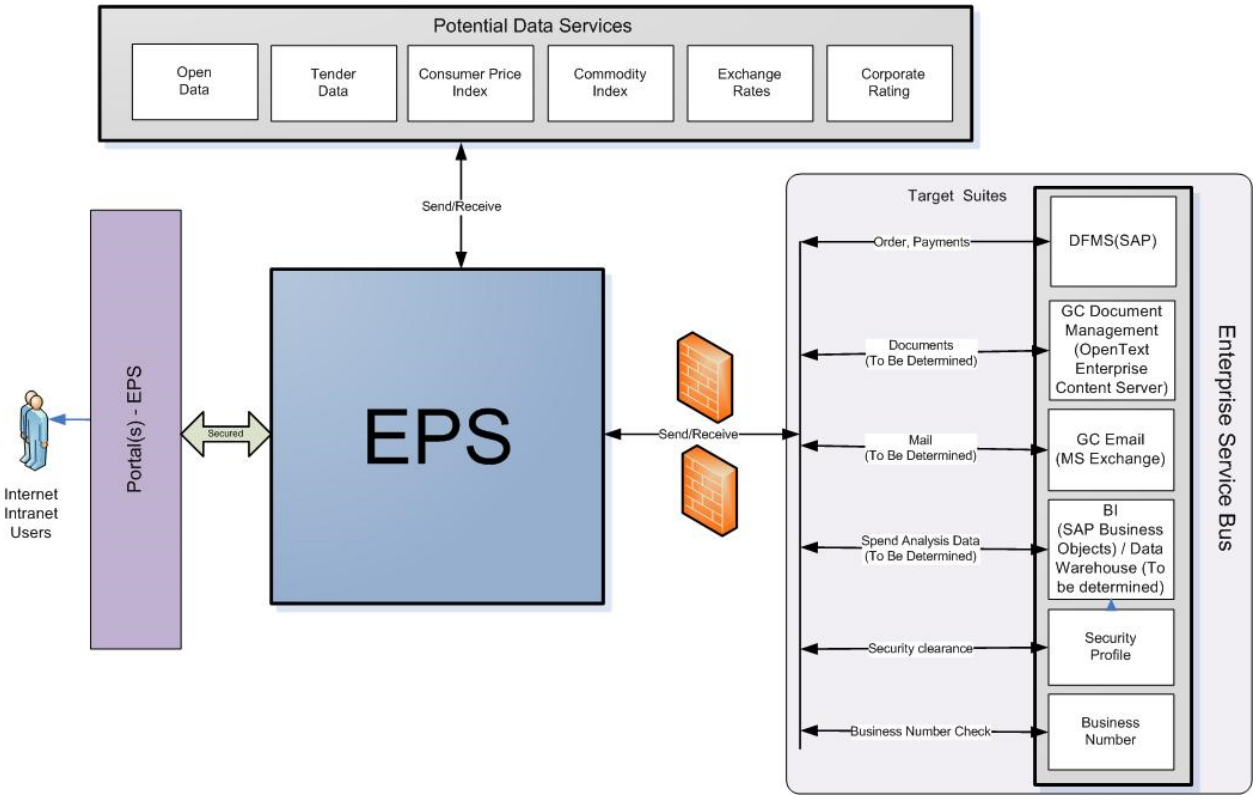
other GC systems. The EPS must support Simple Object Access Protocol (SOAP) based messages and/or file exchanges over ESB as a minimum.

The end-state of EPS must be 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, the EPS may be utilized as the only sourcing and procurement solution for all departments and interoperate with existing enterprise back-office systems, such as Departmental Financial Materiel Management Systems (DFMS) via the ESB.

4.3.2 Solution Vision

Figure 2 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 the EPS will be connected to a number of procurement process support systems and must interoperate, through the Enterprise Service Bus (ESB) with the multiple GC installations of the SAP Department Financial and Materiel Management System (DFMS). The Contractor must ensure that the approach to implementing EPS respects the financial controls and delegation authorities contained within each DFMS. The Contractor will be responsible to configure EPS to communicate with the ESB which will be the central data exchange point between the DFMS and EPS.

Figure 2 - EPS Vision



4.3.2.1 Dependencies

a) **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).
b) **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, Supplier and financial data.

4.3.2.2 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:

a) An intranet or extranet for the key business processes described in Part 3 Functional Requirements.
b) Web services – third party data feeds.
c) Commercially available third party security components such as Public Key Infrastructure (PKI) products.
d) Other procurement systems to transmit and receive information.
e) Other systems containing product information that capture this information for use within its solution.
f) Systems containing supporting information needed to process transactions.
g) Commercially available generic pre-built adapters for interfacing with DFMS.

The Contractor must provide 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 other solution providers can leverage for support in creating integration methodologies, as requested by the GC, for their applications that includes:

a) Enterprise Application Integration tool in a media and format specified by GC.
b) reference documentation (in English and French) on tool usage that includes:
c) Original Equipment Manufacturer (OEM) manuals and guides;
d) instructional documents providing details on controls, methods, data dictionaries, etc.;
e) Best practices and whitepapers;
f) Sample application integration source code;
g) A list of all libraries supported by the EPS;
h) An application compliance testing guide that includes:

i) Test cases that GC partners can use to assess an application's compliance with supported protocols and standards; and
j) A compliance checklist that GC partners can complete to record and report on compliance testing results.

4.3.2.3 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:

a) Open ID connect
b) SAML 2.0
c) JSON
d) Kerberos
e) X.509
f) LDAP
g) OAuth
h) SOAP
i) REST

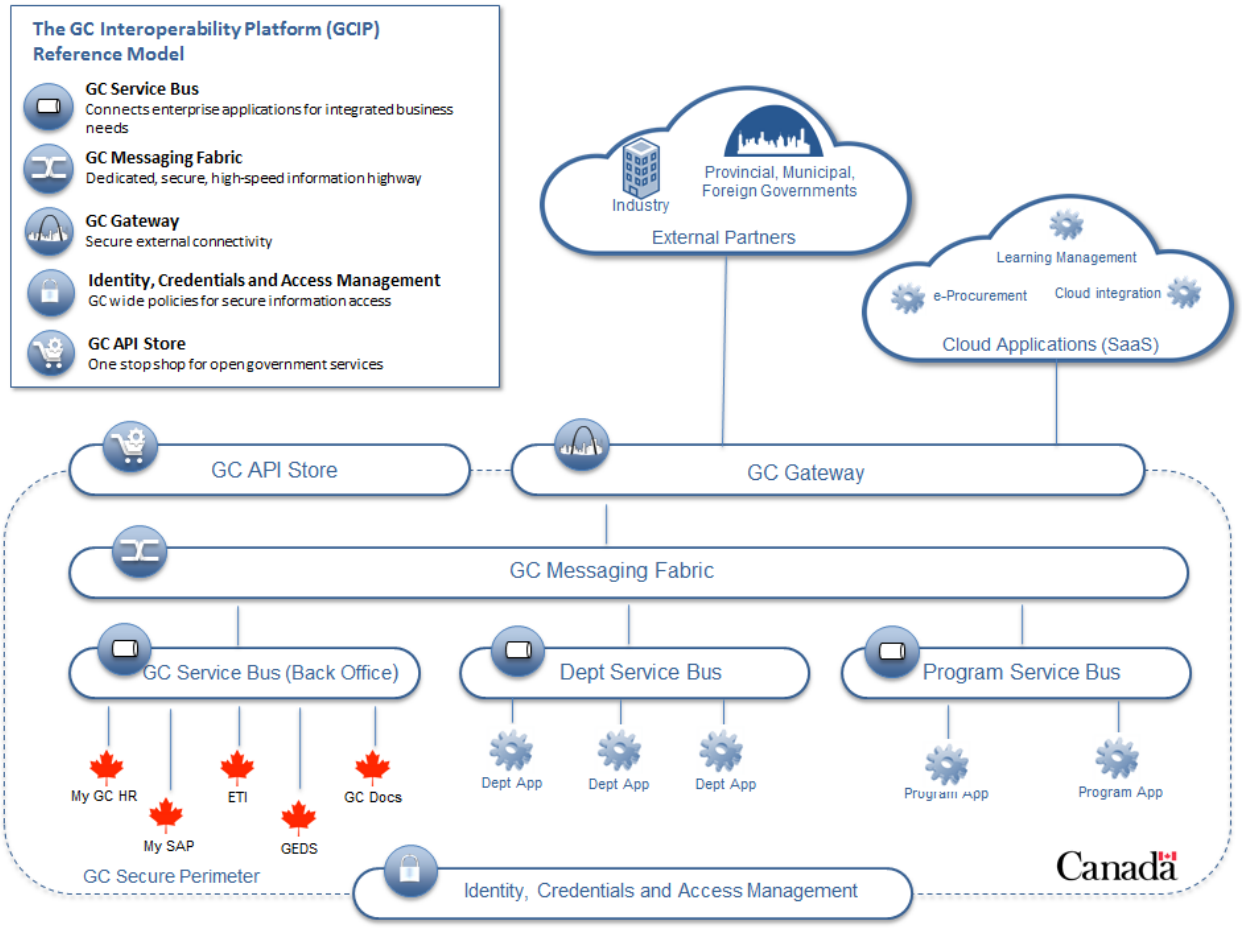
4.3.2.4 Interoperability with GC Back-Office Systems

In support of the GC's strategic plans for application interoperability, the EPS must expose its functionality through an Application Programming Interface (API) that leverages industry-standard API protocols.

GC is in the process of implementing 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. While the EPS must be interoperable with GC data sources through the GC ESB solution, Canada, at its own discretion and if it sees fit, may consider, during the Term of the Contract, other potential solutions for interoperability between the EPS and GC systems.

The following Figure 3 depicts a high level vision of the GC Interoperability Platform.

Figure 3 - High Level Vision of GC Interoperability Platform



4.3.2.5 Requirements for the EPS Interfaces

The following sections describe the interface requirements for EPS

Table 14 – Requirements for the EPS Interfaces

SOW NUM	Requirement
Int.00	The Contractor must deliver a solution that provides the functionality:
Int.01	to create and send information (e.g. Contracts, Purchase Orders) to Suppliers from EPS via notifications (email or alerts on the Portal).
Int.02	to interoperate with DFMS(s) to pull and push data in Near Real-Time using the approved interoperability technology, via ESB, using XML to support the integrated procurement processes
Int.03	to transfer data to the GETS using ESB or Web services.
Int.04	to transfer structured and unstructured data to Open Government Portal.

SOW NUM	Requirement
Int.05	to support dynamic access to Open Data datasets, within GETS and Open Government Portal, through API calls as services.
Int.06	to support the transfer and access of open tender data for all Canadian Public Sectors by aggregating, posting and updating the tender notices in any file format from other jurisdictions.
Int.07	
Int.08	to support the validation of Supplier's business number and legal name in Near Real-Time using XML with the CRA's Business Number Hub system.
Int.09	to receive the exchange rates for specified currencies from a designated source (e.g. Bank of Canada) as per schedule.
Int.10	to receive Consumer Price Index (CPI) data from a designated source (e.g. Statistics Canada) as per schedule.
Int.11	to receive the commodity index feed from a designated source (e.g. Bank of Canada) as per schedule.
Int.12	to receive security clearance data from a designated source on demand at both corporate and resource levels via the ESB.
Int.13	to receive the Supplier's corporate rating from a designated source (e.g. Dunn and BradStreet) on demand using APIs.
Int.14	to support data exchanges to and from legacy systems during the transitional period using GC preferred interface frequency, styles and methods: i. Near Real-Time or batch; ii. Web services / APIs; and iii. XML and/or Flat file.

4.4 EPS TECHNOLOGY REQUIREMENTS

4.4.1 Introduction

The EPS must be a flexible, scalable and adaptable solution that meets changing business needs mostly through managing configurations available within the solution.

The requirements in this section describe what the solution must 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.

The versions and particular brand names of the GC systems will be 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 requested by GC.

4.4.1.1 Compliance

The EPS compliance requirements are stated in *Part 2 Legislative, Regulatory and Policy Requirements*.

Requirements in this section are technology specific compliance requirements that the EPS must facilitate GC's compliance with stated policies, directives and guidelines.

4.4.1.2 Interoperability

The EPS must interoperate with GC's applications and platforms using as a minimum the following:

a) APIs;
b) Export and import of data and content; and
c) Enterprise Messaging/Service Bus.

4.4.1.3 Usability

Usability is the ease of use and learn-ability of the EPS. 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.

4.4.1.4 Reliability

Requirements in this category specify solution capabilities and architecture that in general give a higher level of availability, more maintainable application and higher overall resiliency.

4.4.2 Technical Requirements

Table 15 - General Technical Requirements

SOW NUM	Requirement
Tech.00	**Technical Requirements** The Contractor must deliver a solution that provides the functionality:
Tech.01	to interoperate with GC's applications and platforms using at least the following methods: i. APIs; ii. Export and import of data and content; and iii. Enterprise messaging/Service Bus.
Tech.02	to support the concept of open architecture and allowing accessibility to its services and functionalities through other contractor-provided and/or third-party APIs, Web services, and similar technology.
Tech.03	to support Web pages and Web feeds encoded in UTF-8.
Tech.04	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.05	to support application server "scalability and performance tuning" functionality, through both: i. Scalability built-in: a. An integrated function; and b. an external capability.

SOW NUM	Requirement
	ii. 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.06	to provide distinct staging environment(s) as necessary for the purpose of configuring, testing and training for the new software releases.
Tech.07	to support the capability of versioning of configurations, and the ability to roll back to previous production versions.
Tech.08	to support best practices for securing web services, such as NIST SP 800-95 Guide on Secure Web Services or NIST SP 800-44 Version 2 Guidelines on Securing Public Web Servers.
Tech.09	to support automatically terminating an open web session after a period of inactivity, to be determined by GC.
Tech.10	to support any database to handle manage and protect data up to Protected B level.
Tech.11	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: i. Logical separation of data is preserved; and ii. Physical separation is connected through boundary devices.
Tech.12	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. i. PDF (Adobe PDF); ii. DOC, DOCX(MS word 2007 and above); and iii. XLS,XLSX (MS Excel 2007 and above).
Tech.13	to support the current GC Internet Browser standard – Microsoft Internet Explorer 11, and two previous major versions when the standard changes.
Tech.14	to support the compatibility with major internet browsers on the market(e.g. Firefox, Safari and Chrome).
Tech.15	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.16	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.17	to support the capability of accepting and uploading solicitation documents and attachments with the maximum size possibly greater than 50 Mbytes, and of any formats (e.g. CAD drawings, maps, movies).
Tech.18	to support the capability where a User can navigate directly to an actionable screen from the notification requesting an action, without logging-in again.

SOW NUM	Requirement
Tech.19	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.20	to support the architecture style that enables robust error handling, recovery and notification to Users when online errors occur.
Tech.21	to support best practice web application design principles for usability (e.g. W3 Web Application Best Practices). For example, enabling/disabling buttons, options and flows based on User entered values, reducing needless prompting, etc.
Tech.22	to support a single login within the EPS domain.
Tech.23	Deleted
Tech.24	to support the capability of securing data in transit as follows: i. At least Transport Layer Security (TLS 1.2 or above); and ii. All other cipher suites must be disabled.

4.5 SECURE ACCESS

4.5.1 Overview

This section defines the User authentication requirements for the EPS. In the context of EPS, secure access is the ability to permit or deny User access to resources within the EPS.

The EPS must provide secure access for 3 general groups of Users: GC Users (e.g. Government employees), non-GC Users (e.g. Suppliers, Broader Public Sector), and System Administrators (e.g. Service Operators).

4.5.1.1 Group 1: GC users

The EPS must interoperate with the GC's Internal Centralized Authentication Service (ICAS).Currently, GC has only defined the Credential Management component of this solution. The following components available with credential management are:

a) Managed user credentials;
b) Authentication service for protected and non-protected information; and,
c) 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.

Canada is in the process of acquiring a new ICAS to replace myKey. Once the ICAS is ready, Canada may exercise a Task Authorization for integration between the EPS and the ICAS. Canada may consider an

alternative to myKey as an interim solution to the GC's ICAS provided that it meets the required Level of Assurance.

4.5.1.2 Group 2: NonGC users

There is a corresponding external credential that is available to NonGC users which is called "GCKey". GCKey is a Government of Canada Branded secure credential service supported by Shared Services Canada. GCKey or a Contractor supplied equivalent must be used for secure access to EPS by all nonGC Users (e.g. Suppliers including international Suppliers and the Broader Public Sector when required). Canada maintains the option to choose either the GCKey or the

Contractor-supplied equivalent, if available, to be used for secure access to EPS by all non-GC Users under the Contract.

4.5.1.3 Group 3: System Administrators

The Contractor must deliver, enable and support an identity, credential and access management service for all Contractor resources.

Please refer to Annex 2 – Security and Privacy 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).

GCKey: https://clegc-gckey.gc.ca/j/eng/AB-01

Table 12 -Secure Access Requirements for GC Users

SOW NUM	Requirement
SecureInt.00	**GC 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 EPS using the GC's Internal Centralized Authentication Service (ICAS) (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 across multiple workstations or devices.

Table 17 - Secure Access for non-GC Users

SOW NUM	Requirement
SecureExt.00	**non-GC Users** The Contractor must deliver a solution that provides the functionality:
SecureExt.01	to integrate with the GC's GCKey for external resources (non-GC) or a Contractor-supplied equivalent.
SecureExt.02	to provide a self-registration interface. The interface must allow for an approved User with delegation of authority within a Supplier/BPS organization to approve or deny other Users registering within that Supplier/BPS organization (to allow multiple Users within a Supplier/BPS organization).
SecureExt.03	to link a GCKey credential to an User account.
SecureExt.04	to authenticate a User using GCKey at logon to the EPS.

4.5.2 Key Management Service

The Government of Canada has a requirement for an EPS Key Management Service (KMS) that supports on-line delivery of EPS. The EPS provisioned KMS based services must assist the GC in managing and controlling access to their EPS through the provision of standardized registration and authentication processes.

The KMS provides the identities and credentials for the purposes of EPS user authentication and data encryption, as required, within the EPS. The KMS will be the single source for the issuing and management of EPS based PKI credentials. This service would, through use of KMS credentials (PKI Keys), provide secure access to EPS, as well as data encryption, and the other advantages presented by use of a common service. Additionally, the KMS must be able to extend the use of the PKI-based identities and credentials across the whole of the EPS as proposed for the GC.

The KMS's main component is the Certification Authority (CA), a management node of the EPS KMS Public Key Infrastructure (PKI) that provides identity-based and anonymous-based PKI security services to EPS and its users.

The KMS must comply with applicable technical, management, and operational security requirements as detailed within Annex 2.

PART 5: NON-FUNCTIONAL REQUIREMENTS

5.1 CONTEXT

This part is to identify outcomes or requirements that are applicable across all aspects of the EPS.

5.2 HIGH LEVEL COMMITMENTS

5.2.1 Ability to Adapt to Change

The EPS must be able to adapt and accommodate to change 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**:**

a) 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;
b) Adding a new or modifying an existing data element to accommodate new reporting requirements or changes to existing data dictionaries;
c) Adding new or modifying the existing content of communications messages;
d) Importing and/or exporting information with new or existing systems or services (i.e. importing new Supplier risk information feed into the Supplier relationship management environment); and
e) 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 5 Non-Functional Requirements clearly lays out requirements for a flexible solution that is able to evolve over time without incurring significant information technology change management costs.

5.2.2 Solution Flexibility

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

a) Document process changes;
b) Maintain complete records of accounts impacted by the change; and
c) Develop ad hoc reports to quantify and qualify changes as a result of the modified or suspended processing.

5.2.2.1 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 workflows, data fields, processes, and configurations accordingly, often with short turnaround times.

5.2.3 Solution Usability

The Contractor must adopt and leverage best practices in solution design, including but not limited to:

a) Ensure consistent and standardized user interface in the EPS.
b) Guide the Users by providing context sensitive help messages and visual process maps available when requested by GC.
c) 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.
d) 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.
e) Smooth integration with productivity tools and desktop environment, such as drag and drop capability with MS Office products suite.
f) Allow a User to create hyperlinks to any document so that it can be referenced anywhere within the solution.
g) 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.

5.2.4 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:

a) Avoid unnecessary collection of duplicate information, reconcile inconsistencies and ensure data quality;
b) Ensure that information is complete, accurate, current, relevant, and understandable;
c) Support access to information subject to policy and legal requirements;
d) Prevent unlawful access to information;
e) Safeguard information against loss, theft and damage;
f) What and how information is to be captured and used;
g) How long a program or service will operate; and
h) How long the information will be needed for operational and legal / evidential purposes.

5.3 SERVICE DELIVERY IN BOTH OFFICIAL LANGUAGES

As required by the *Official Languages Act*, the GC has an obligation to provide service delivery in the GC's two official languages: English and French. The Contractor must ensure all user-facing components of EPS applications, services, 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) are available in both official languages, and must:

a) Provide materials for any User in both official languages.
b) Personal communications to Users must be provided in the User's language of choice, with English as the default language if the User has not indicated a preference.
c) Maintain a record of User's language preference so that all personal communications are received in their language of choice.
d) Ensure that all user-oriented communication materials are available for distribution in both official languages.
e) Ensure EPS is available in the official language of the User's choice. This includes all user-facing.

5.3.1 Additional Official Language Obligations Applicable to Procurement

When procurements are public, 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 documents must be provided in both official languages. Additionally, all public GC solicitations must be bilingual.

As such, the EPS must enable Users to:

a) 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 or both official languages.
b) 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.
c) Publish Supplier's questions and the responses in both official languages during bid solicitations.
d) Search and purchase in both official languages - meaning catalogues must be capable of being created with attributes in both official languages for the same product.

5.4 SECURITY AND PRIVACY

5.4.1 Security

Annex 2 – Security and Privacy will detail security requirements and the Security Requirements Traceability Matrix.

The Contractor must ensure that the EPS datacenters, EPS software, EPS middleware, the EPS service desk, Security Operations Centre (SOC) and Network Operations Centre (NOC) infrastructure and Data for the entire EPS must reside in Canada and/or countries with which Canada has International Bilateral Industrial Security Instruments (IBISI).

The Contractor must ensure that all Work under the Contract (including SOC, NOC and service desk) performed by Contractor personnel, whether through subcontract or otherwise, be performed within Canada, countries with which Canada has IBISI, European Union and/or NATO countries.

The Contractor must ensure any business entity conducting Work under the Contract have a physical location within Canada, countries with which Canada has IBISI, European Union and/or NATO countries and be incorporated or legally authorized to do business and operate or registered where the local legislation requires such registration.

5.4.2 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.

The Contractor must safeguard all personal and protected information, including, but not limited to, the following:

a) Supplier identification information (e.g. names, addresses, company profiles, résumés, work experience, previous contracts completed, and clients).
b) Supplier financial data (e.g. banking information).
c) Procedures, forms, computer systems and data file layouts, and Internet Web sites, etc.
d) Contact information (including business name), biographical information, educational information, financial information, evaluations/assessments, other identification number (e.g. Business Number) and signature.

5.4.3 Protected Information

The Contractor must:

a) Be responsible for the safekeeping, protection and privacy of this information, and upon close-out of the Contract, returning all information to the GC;
b) 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
c) 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:
    i. Ensure that the quality, accuracy, completeness and integrity of the data within the system is always maintained through the use of appropriate validation measures;
    ii. Ensure that the consistency of the data is both reconcilable and auditable;
    iii. maintain a multi-channel history of information sent or received, information exchanged, and account updates performed by or on behalf of the client;

iv. 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

v. Ensure any destruction of records is completed following the standards set out in the *Library and Archives Act* and EPS Disposition Authority.

5.4.4 IT Security Certifications

The Contractor must maintain any certification and audit standards, provided as part of its bid, during the entire Term of the Contract.

Prior to enabling any credit card processing through EPS, if applicable, the Contractor (and/or their sub-contractor) must provide a valid PCI DSS Level 1 certificate and must maintain the PCI DSS Level 1 certification throughout the entire period in which credit card processing occurs through EPS.

5.5 COMMUNICATIONS

The EPS must be able to 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 Users, the EPS must also offer multiple service delivery channels including call centre, Automated Attendant (AA), e-mail, knowledge base/self-help, and user service Portal.

Regardless of the channels selected by Users for account management and communications, the Contractor must integrate User contact and service delivery channels so that the same information "set" is modified, updated, and accessed consistently. The Contractor must apply, to the greatest extent possible, the principle of first contact resolution to User 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 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.

5.5.1 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 must 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 appropriate 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 provide 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 the EPS to Users as required. The Contractor must provide a repository of pre-approved communications messages and standard communications templates that GC has the ability to configure and access to generate these communications to Users through the EPS.

5.6 SERVICE DESK

5.6.1 Service Manager

The Contractor must provide a Service Manager that must be available to meet with GC's representatives during business days from 07:00 to 18:00 EST to deal with release implementation activities, release maintenance and release window scheduling, service quality, management services escalation (Incidents), and service reporting, and be reachable outside of business hours for high priority Incidents, urgencies, and security Incidents.

5.6.2 Service Desk Requirements

The Contractor must provide and maintain a bilingual (in English and in French) service desk accessible by all Users (including Suppliers) to provide support in the use of EPS and to resolve Users' technical challenges including functional or navigational questions. The service desk must collaborate with GC technical support staff in the resolution of EPS issues relating to GC systems.

The service desk must route inquiries regarding GC procurement business, policies and processes to a service desk specified by the GC.

5.6.2.1 General

The Contractor must:

a) provide all necessary resources and staff to operate the bilingual service desk.
b) provide a toll-free telephone number for the service desk for Users within Canada.
c) have support processes defined and practiced; including Incident Management, problem management, change management and escalation process.
d) generate a service desk performance report to demonstrate the degree of adherence to Service Level Requirements (SLRs) as defined in *Section 6.13 Service Level Requirements*.

e) the Service Desk support, when interacting with EPS users, must be in both official languages. The elements in which Service Desk support does not interact with EPS users does not have to be in both official languages.
f) provide expert Tier 1, Tier 2, and Tier 3 assistance for inquiries about the features, functions and usage of hardware and software.
g) identify, escalate (e.g., Tier 2 and Tier 3 escalation), manage Incident Resolution and Close Incidents and Service Requests, including those escalated to Third Parties.
h) design and deploy a functional escalation model that provides for Incident resolution. It must escalate unresolved Incidents to another Tier of support for resolution and collect required information from the caller before escalation.
i) provide appropriately trained service desk staff for Tier 1, Tier 2, and Tier 3 support to meet technical requirements.
j) provide a closed-loop process for Incident Management, which includes informing the User of status changes or contacting the User for more information as required.
k) the proposed ITSM service or system must support communication with other managed service providers (MSPs) and GC's ITSM, at the application programming interface (API) level.
l) develop, document and maintain service desk Operations and Administration procedures that meet the requirements.
m) provide additional Resources, as needed, during planned and unplanned critical events.
n) track/manage/report service desk utilization.
o) maintain and provide escalation contact list(s) for all Service Tiers (including Third Parties).
p) issue broadcasts or other notices to provide status updates, as required, for planned and unplanned events.
q) . provide User access to Service Requests and Incident reports as requested by the GC.
r) develop and execute procedures for conducting User Satisfaction surveys in accordance with the Service-Level Requirements.

5.6.2.2 First Point of Contact

The Contractor must act as a first point of contact for all User Incidents, requests and general communication and must provide technical related support including:

a) Restoring 'normal service operation' as quickly as possible in the case of disruption;
b) Improving User awareness of IT Incidents and to promote appropriate use of IT services and resources;
c) Assisting other IT functions by managing User communication and escalating Incidents and requests using defined procedures;
d) Resolving incidents including hardware, system software, and network issues
e) Responding to application incidents and provide "how to" support; and
f) Provide password support for Contractor provided credentials (if applicable), including self-service password reset capabilities, requests for account privilege change requests, requests for User account activation, suspension and termination.
g) Provide First Point of Contact (FPOC) call-in access via a toll-free number for all service desk Services described in this SOW.

h) Provide multiple alternative communications channels, including voice messages, email and intranet.

5.6.2.3 Delivery Channels

The Contractor must provide a service desk that is accessible as per table 5.6.4.4 Service Desk Tiers and Responses Levels in all Canadian time zones using service delivery channels including:

a) **Phone:** Providing a phone line allowing Users to speak directly with service desk support to submit and resolve service requests.
b) **Automated Attendant (AA):** Develop and implement the Automated Attendant (AA) service channel. This service will present Users with an appropriate array of self-service options. The AA service must be provided in both official languages 24 hours a day, 7 days a week. Users must have the option of speaking to service desk support at any point during operating hours. The AA must include:

   i. Prompt response: to answer all calls on the first ring
   ii. User service: 24 hours a day, 7 days a week
   iii. Call redirection: use a simple menu to route callers to the appropriate telephone number or recorded information without any personal assistance. Recorded information can be updated at any time from any telephone, and is password protected.
   iv. Message service: hold the call for a specific extension if it rings busy, announce the caller's position in queue and offer the options to stay in queue, leave a message, or hang up and try again later.

c) **Email:** Providing an e-mail address or web form allowing Users to use their email program to submit service requests. The Contractor must provide confirmation and notifications via e-mail to all Users who contact the service desk via e-mail.
d) **Live Chat:** Providing a chat session, allowing Users to open a text dialogue.
e) **Self Service:** In addition to providing Users the ability to attempt self-resolution via accessing a knowledge base, the Contractor must
   i. Develop, document and maintain the Self-Help Support.
   ii. Implement Self-Help Support capabilities that enable Users to perform self-service, including administrative functions, “how to” support through User access to knowledge bases and online Incident status checking.
   iii. Provide Self-Help support in both official languages.
f) **Persons with Disabilities:** The GC is committed to ensuring public accessibility for 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 as required. The Contractor must ensure that service desk technology is updated and incorporated into the overall client services.
g) **Frequently Asked Questions:** Allows both the Contractor and Users to reference a list of common questions and answers that can leverage a knowledge base.

5.6.2.4 Service Desk Tiers and Operating Hours

Table 18 - Service Desk Tiers and Operating Hours

Tier	Standard Operating Hours in Eastern Time Zone (ET)
Tier 3	Mon-Fri 09:00-17:00
Tier 2	Mon-Fri 07.00-19.00
Tier 1	Mon-Fri 07.00-19.00

Tier 1 – is the initial support level responsible for basic customer issues and provides generalist support based on a broad understanding of the product

Tier 2 - is a more in-depth technical support level than Tier I and the technicians are more experienced and knowledgeable on the product. They are responsible for assisting Tier I personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues

Tier 3 - is the highest level of support and responsible for handling the most difficult or advanced problems. These individuals are experts in the product and are responsible for not only assisting both Tier I and Tier II personnel, but with the resolution of new or unknown issues.

5.6.2.5 Priority Levels

The following table defines the priority levels of incidences:

Table 19 - Priority Levels

Priority Level 1: Emergency/Urgent – Critical Business Impact or National Interest	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. No workaround available. Examples: ■ Major application problem (e.g., cataloguing, sourcing, etc.) ■ Severe disruption during critical periods (e.g., fiscal year end processing) ■ Network outage ■ Security violation In addition, Priority Level 1 must be assigned to Incidents pertaining to national interest
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 at a significantly reduced capacity or functionality. A workaround may be available, but is not easily sustainable. Examples: ■ Major data/database or application problem ■ 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 Users or the EPS and/or service is degraded. A workaround may be available.
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

5.6.2.6 Incident Management

The Contractor must manage incidents to ensure the rapid restoration of services following an unplanned deviation within the Contractor's business and IT environments, including:

a) Recommend Service Request and Incident Management procedures derived from the ITIL or ISO processes
b) 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 Users).
c) Escalate to Tier 2 and Tier 3 support 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
d) 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 Users).
e) Provide an end-to-end Incident identification, escalation, transfer, resolution (management) and closure process, including Incidents escalated to Third Parties.
f) Receive, track, answer and resolve, or monitor to closure, User and technical staff calls.
g) 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.
h) Document solutions to re-occurring incidents in the knowledge database with the exception of security incidents.
i) Verify acceptance of services by contacting the User to confirm results and level of satisfaction.
j) Ensure that recurring Incidents that meet defined criteria are reviewed using Root Cause Analysis processes.
k) Provide authorization for closing of service requests and service desk Incidents.
l) Provide to GC complete and continuous access to all requests and incident closure information and data such as:

i. Incident receipt;
ii. Incident identification;
iii. Incident prioritization;
iv. Incident management;
v. Incident assignment;
vi. Incident logging, tracking and updating methods; and
vii. Incident resolution and closing.

5.6.2.7 Service Desk Reporting

The service desk must include a set of standard reports (e.g. incident management reporting, problem management reporting and service reports) that have already been configured for quick-and-easy use.

5.7 SERVICE MANAGEMENT

Service Management is the strategic approach to designing, delivering, managing and improving the way information technology (IT) will be used within EPS across the GC. The goal of Service Management is to ensure that the right processes, people and technology are in place so that the EPS can meet its business goals. Service Management is associated with Information Technology Infrastructure Library (ITIL), a framework that provides best practices for aligning IT with business needs.

The Contractor must manage its IT services and deploy a set of specialized resources and capabilities equivalent to those prescribed by the ITIL framework as a source of best practice in service management. The framework must emphasize the importance of coordination and control across the various functions, processes, and systems necessary to manage the full life cycle of IT Services including the Strategy Development, Design, Transition, Operation and Continual Improvement—The IT Service Management Lifecycle.

The Contractor must provide audit reports conducted by an independent organization (internal or external) to demonstrate alignment with best practices and actions taken to address gaps.

The Contractor must adapt the ITIL Guidance (or similar framework) to support the EPS environment, and must continually deploy these practices for the duration of the Contract. The Contractor must provide audit reports to the Project Authority to demonstrate continued compliance as requested by the GC.

5.8 WEB ACCESSIBILITY

In accordance with the Standard on Web Accessibility, the Contractor must ensure each web page of the EPS meets all five WCAG 2.0 conformance requirements. Conformance requirement level 1 must meet level AA conformance in full. Prior to the commencement of any operational activity (e.g. pilots, go-live, etc.), Canada will assess the EPS's compliance with the WCAG 2.0 conformance requirements. If the EPS fails to achieve full compliance with the WCAG 2.0 conformance requirements, the contractor must develop a strategy and timeline for reaching a full compliance score for approval by the GC and must take corrective actions to achieve compliance. During the compliance assessment, Canada may determine that critical elements of the WCAG 2.0 conformance requirements must be met prior to the commencement of any operation activity. Once corrective

actions have been completed for the critical elements, Canada will reassess to ensure full compliance has been met.

PART 6: MANAGEMENT AND OVERSIGHT

6.1 CONTEXT

Part 6 describes the GC's oversight and contract management requirements and expectations. GC's overall aim is to ensure a consistent approach to training, communications, transition and steady-state operations. GC will work jointly with the Contractor to establish an active and ongoing relationship that is essential to achieving the overall EPS objectives.

6.2 GOVERNANCE EXPECTATIONS – MANAGEMENT APPROACH

The Contractor must work collaboratively with the GC to develop a governance and Contract management structure that meets the GC's expectations and requirements of this Contract.

6.2.1 Management/Governance Principles

The management and governance principles must be defined within the context of the following overarching principles:

a) **Stewardship**: activities and processes to safeguard money, assets, databases and other knowledge and data assets and protect them against losses, misuses and waste;
b) **Transparency:** measureable outcomes-based results, performance metrics and reporting;
c) **Efficiency/timeliness:** a solution that demonstrates successful, efficient change management and results in improved service delivery; and
d) **Flexibility:** a solution and delivery of services that demonstrates innovation with a focus on flexibility to accommodate multi-layered change and continual service improvement.

6.2.2 Planning Principles

For each plan, the Contractor must:

a) Consult and collaborate with the GC in the development of the plan and incorporate the considerations, dependencies, constraints, and stakeholders raised by the GC;
b) Use a logical multi-phased sequence, which would allow the proper level of communications to all stakeholders, both internal and external, in order to support them through a mature change management process of iteratively moving to an EPS;
c) Include a Responsible, Approver, Consulted, and Informed (RACI) chart to identify the roles and responsibilities for key Contractor, GC and any third party members involved for the successful execution of the plan;
d) Provide a list of task dependencies;
e) Not create unnecessary dependencies on GC's review and approval;
f) 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;

g) Identify each Contract deliverable as a milestone;
h) Schedule tasks in parallel to the maximum extent possible;
i) Provide a list of planning assumptions;
j) Identify risks including:
    i. categorization of each risk;
    ii. probability of each risk;
    iii. impact if the risk materializes;
    iv. mitigation measures and risk response;
    v. monitoring measures; and
    vi. risk assignment.

6.2.3 Project Management Office

Within 10 business days of Contract Award and until the acceptance of the delivery of the Milestones in *Section 6.10 Milestones*, the Contractor must staff and operationalize a project office in the National Capital Region to support the execution of the Contract and to:

a) Ensure overall coordination of all project related activities under the EPS Contract;
b) Manage the resolution of EPS project issues, problems and complaints, and escalate and prioritize project issues as requested by the GC;
c) Provide a project manager who will function as the GC's single point of contact and Contractor's representative for the Project Management Office; and
d) Provide a telephone number in the National Capital Region (NCR) and email address to contact the Project Management Office from 8:00 to 17:00 ET, during business hours.

6.3 PROJECT PLANS

6.3.1 Preliminary Project Plan

The Contractor must submit a Preliminary Project Plan within 5 business days of the Kick-Off Meeting described in *Section 6.9.1 Kick-Off Meeting* for approval by GC that identifies a schedule to complete the plans and Work required in this SOW.

6.3.2 Project Management Methodology and Plan

The Contractor must provide to the Project Authority a draft project management plan, which includes the Implementation Plan that was proposed as part of the Contractor's bid submission, within 10 business days following approval of the preliminary project plan for review and approval by the Project Authority.

The project management plan must address and integrate all the project management knowledge areas as defined in PMBOK edition 5 or PRINCE2 and must include the following:

a) Executive summary description of the EPS and its services;
b) Organizational plan that includes management structure, organizations, and detailed descriptions of roles and responsibilities and qualifications of key project personnel and subject matter experts. The

descriptions must address the education; training; experience pertinent to the function; availability and replacement schedule; and responsibility;

c) 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. The Contractor must indicate what additional resources they would have available for deployment in case the level of effort being required beyond that which was originally estimated for the above;

d) Contract Work Breakdown Structure (CWBS) at the activity level 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;

e) Change 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 Work performed by subcontractors;

f) Subcontract Management Plan that identifies the working relationships between the different subcontractors involved in the Work and relationship with the Contractor. Relations with subcontractors must be described in detail. Methods for control and monitoring of subcontractor performance must be described. Methods by which subcontractors are selected, and conditions under which a subcontractor may be replaced must be detailed. The Contractor must define the subcontractors' interfaces with functional areas of the Contractor organization, and their participation in project progress review updates with the Project Authority;

g) A Project Schedule 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 change control system;

h) 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 Contractor, and GC; and a description of the formal design and configuration review process including roles of subcontractors;

i) Quality Assurance (QA) Plan that includes an approach to formulating and enforcing work and quality standards, and reviewing work in progress. The plan must address, but not limited to:

    i. A detailed description of the Contractor's QA methodology, processes and procedures, and its alignment with a recognized quality management system;

ii. QA requirements for the implementation and all transition activities, including proposed baseline performance requirements;
iii. A description of the QA organization;
iv. The collateral demands on GC project staff time for participation in the overall QA program,
v. The interfaces between the contractor's QA/QC functions and those of its subcontractor(s), and how the responsibilities are allocated;
vi. Procedural and contractual remedies for recovery of quality problems must be specified for consideration by the Project Authority as components in the final QA program.

j) 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;

k) 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; and

l) Performance management system including metrics that are based on well-established project management methodologies as defined in PMBOK 5th edition or PRINCE2, to track the scope, schedule, and cost parameters.

6.3.3 Relationship Management Plan

The Contractor must provide to the Project Authority a draft Relationship Management Plan within 15 business days following the Kick-Off Meeting for review and approval by the Project Authority.

As a minimum, the Relationship Management Plan must include the Contractor's approach to:

a. GC – Contractor management of the business relationship;
b. Multi-year planning;
c. Priority setting;
d. Resource management;
e. Communications between the delivery partners;
f. Communicating upcoming changes and their potential impact to Users;
g. Multi-channel relationship management;
h. Issue management and resolution;
i. reporting and working with the GC to resolve service standard exceptions, problems and issues, and documentation;
j. Joint planning;
k. Proposed terms of reference(s) for any joint committees (including frequency of meetings);
l. change management, including prioritization, planning and reporting (roadmap);
m. 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;

n. 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
o. Quality assurance - roles and responsibilities in ensuring quality is maintained in client services and account management processes.

6.4 PRIVACY MANAGEMENT

6.4.1 Privacy Management Plan

The Contractor must provide to the Project Authority a draft Privacy Management Plan within 45 business days following Contract Award for review and approval by the Project Authority.

As a minimum, the Privacy Management Plan must include:

a. Contractor's privacy protection strategies and detail of exactly how the Personal Information will be treated over its life cycle;
b. how the Personal Information will be collected, used, retained, disclosed and disposed only for the purposes of the Work specified in the Contract;
c. how the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;
d. the privacy breach protocol and details on how any privacy breaches will be handled;
e. how the Contractor will ensure that Canadian Privacy requirements, as outlined in the Privacy Act, the Access to Information Act and Library and Archives of Canada Act, will be met throughout the performance of the Work and for the duration of the Contract;
f. any new measures the Contractor will implement in order to safeguard the Personal Information and the Records in accordance with their security classification;
g. how the Contractor will ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification; and
h. how the Contractor will ensure that their staff is trained on privacy and privacy related principles.

6.4.2 Privacy Management Plan delivery

The Contractor must implement the Privacy Management Plan (all processes, procedures, roles, responsibilities etc.), and any subsequent annual updates.

The Contractor must provide to PWGSC within 30 business days of a request by the Project Authority, evidence not older than 12 months (e.g. test results, evaluations, and audits) that the Privacy Management Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting the GC's privacy requirements.

If changes to the EPS environment are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by the Project Authority, the Contractor must provide PWGSC with sufficient detail to support an update to the Privacy Impact Assessment, and obtain approval from the Project Authority for the anticipated change.

The Contractor must provide within 60 business days of Contract Award a privacy awareness guide instructing the Contractor's resources regarding the use of the Personal Information provided by the GC about the Users.

6.4.3 Privacy Impact Assessment

The Contractor must provide the requested assistance to the GC in creating the Privacy Impact Assessment in accordance with the TBS Directive on Privacy Impact Assessment (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308) and provide the following information within 20 business days of a request by PWGSC:

a) business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;
b) a list of the Personal Information used by the Contractor in connection with the Work and the purpose of each Personal Information item;
c) how the Personal Information is shared and with whom;
d) a list of all secured locations where hard copies of Personal Information are stored;
e) a list of all secured locations where Personal Information in machine-readable format is stored (e.g., the location where any server housing a database including any Personal Information is located), including back-ups;
f) a list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by the Contract;
g) any privacy-specific security requirements or recommendations that need to be addressed;
h) a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and
i) results of consultations (if any) from a privacy impact assessment review by the Office of the Privacy Commissioner of Canada (OPC) with signoff by OPC

The Contractor must implement the recommendations from the Privacy Impact Assessment based on a schedule approved by PWGSC.

If changes to EPS are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by the PWGSC, the Contractor must provide PWGSC with sufficient detail on the changes to support an update to the Privacy Impact Assessment, and obtain approval from Project Authority for the anticipated change.

The Contractor must provide a privacy awareness communications kit to Contractor resources involved in the EPS that provides an overview on the use, collection and disclosure of Personal Information.

6.5 IT SECURITY MANAGEMENT

6.5.1 IT Security Operations Centre

The Contractor must provide a Security Operations Centre (SOC), prior to the deployment of any functionality to production, 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 the EPS security Incidents.

The Security Operations Center (SOC) must:

a) coordinate security Incidents responses in close coordination with GC;
b) include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year and answered using the official languages of the GC (French and English) as requested by the caller;
c) act as a point of contact for communications with GC representatives for security Incidents;
d) not impact operations of the EPS in case of a Contractor SOC failure; and
e) 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 collaborate with PWGSC's Information Protection Centre for activities that include: integration of processes; oversight; security Incident handling and response; and auditing.

The SOC must accept emails from 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.

6.5.2 IT Security Plan

The IT Security Plan must describe how the security requirements will be addressed in alignment with the PWGSC Security Assessment and Authorization (SA&A) process, as described in section 6.6 PWGSC Security Assessment and Authorization (SA&A) Process of this SOW. The Contractor must submit the IT Security Plan within 45 business days of contract award. 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, the controls at each Gate must be refined by the Contractor, to the satisfaction of the GC, during the SA&A process.

6.5.3 IT Service Continuity Plan

The Contractor must update, as requested by the GC, the IT Service Continuity Plan submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised IT Service Continuity Plan for approval.

6.5.4 Technical Deployment Model

The Contractor must update, as requested by the GC, the Technical Deployment Model submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised Technical Deployment Model for approval.

6.5.5 Technical Architecture Diagrams

The Contractor must update, as requested by the GC, the Technical Architecture Diagrams submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised Technical Architecture Diagrams for approval.

6.5.6 Technical Integration Approach

The Contractor must update, as requested by the GC, the Technical Architecture Approach submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised Technical Integration Approach for approval.

6.6 PWGSC SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) PROCESS

The SA&A process must be completed in its entirety, and to the satisfaction of the GC, prior to the commencement of any operational activity (e.g. pilots, go-live, etc.) including production transactions and data. Thereafter, with each release or change management implementation, the SA&A process must be repeated and documented. Should Canada discover, through the SA&A process, security risks that are deemed unacceptable by Canada, Canada, at its own discretion, may exercise any rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default).

6.6.1 Security Assessment and Authorization Gate 1

The Contractor must complete the following Work for SA&A Gate 1:

a) Security High Level Service Design (SHLSD); and
b) Security Requirements Traceability Matrix (SRTM).

All Work will be subject to approval by the Project Authority.

6.6.1.1 Security High Level Service Design

The Contractor must provide a SHLSD 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; and
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.

6.6.1.2 Security Requirements Traceability Matrix

The Contractor must provide a SRTM to GC that includes for each requirement in Annex 2 – Security and Privacy:

a) the security requirement identifier (E2.xx as identified in the Annex 2 for each of the security requirements);
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 the GC 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 the GC to confirm that the security safeguards satisfy the security requirements

6.6.2 Security Assessment and Authorization Gate 2

The Contractor must complete the following Work for SA&A Gate 2, 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.

6.6.2.1 Security Detailed Service Design (SDSD);

The Contractor must provide a SDSD 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.

6.6.2.2 Updated Security Requirements Traceability Matrix

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 the GC 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 the GC to confirm that the security safeguards satisfy the security requirements.

6.6.2.3 Change Management Procedures

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;
i) procedures that the Contractor will use to accept modified or newly created configuration items; and
j) a Change Management log.

6.6.2.4 Operational Security Procedures

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.

6.6.2.5 Security Installation Procedures

The Contractor must provide Security Installation Procedures details 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).

6.6.3 Security Assessment and Authorization Gate 3

The Contractor must complete the following Work for SA&A Gate 3, 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;

6.6.3.1 Security Installation Verification Plan

The Contractor must provide a Security Installation Verification Plan to GC that must include:

a) the security verification approach;
b) the GC 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.

6.6.3.2 Security Installation Verification Report

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.

6.6.3.3 Security Integration Test Plan

The Contractor must provide a Security Integration Test Plan as part of the IT Security Plan submission to GC for approval 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.

6.6.3.4 Security Integration Test Report

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.

6.6.3.5 Vulnerability Assessment Plan

The Contractor must provide a Vulnerability Assessment Plan for GC approval and 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.

6.6.3.6 Vulnerability Assessment Report

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 the GC;
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; 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.

6.7 ORGANIZATIONAL CHANGE MANAGEMENT AND COMMUNICATIONS

6.7.1 Organizational Change Management Strategy

The Contractor must provide to the Project Authority a draft Organizational Change Management Strategy within 5 business days following the Kick-Off Meeting for review and approval by the Project Authority.

As a minimum, the Organizational Change Management Strategy must include a high level change strategy based on an assessment of the project, risks and stakeholders which includes:

a) Assessment to understand the change (Context of Change, Impact of Change, Change Agility [readiness]), project and change risk assessment, and high-level stakeholder identification and mapping;

b) "Best Fit Change Strategy" that identifies the right overall concept for delivering change based on the assessment. This should cover benefits of the approach, how to involve stakeholders, and sustainability;
c) Discussion of transition approach for Users based on leading practices;
d) Identification of change levers available to the project team;
e) Change resourcing expectations based on project phases and milestones;
f) Project Team health assessments; and
g) People readiness assessments tied to each go-live.

6.7.2 Change Management Plan

The Contractor must provide to the Project Authority a draft Change Management Plan within 10 business days following the approval of the Change Management Strategy for review and approval by the Project Authority.

As a minimum, the Change Management Plan must be a detailed plan that includes:

a) High level awareness communications plan as per *Section 5.5 Communications* which includes:
    i. communicating program benefits of the EPS;
    ii. communicating how the GC readiness activities will be accomplished;
    iii. communicating how Users can support the GC;
    iv. transition effort;
    v. post-migration assessment to aid in future transition activities; and
    vi. a timeline and key messages and mediums for each stage of the project.
b) Change Leadership engagement: confirming leadership buy-in, creating change advocates, providing coaching and tools for their role in driving adoption;
c) Change Network: Develop a change advocate network within PWGSC and then across GC departments, attain leadership engagement for active support and driving change;
d) Identifying barriers to change and possible actions;
e) Identifying quick wins;
f) A set of processes to ensure the change is adopted and sustained in the long term;
g) Processes and procedures to institutionalize the change;
h) Alignment with training timelines, communications, and approaches;
i) Alignment with the Supplier Enablement Plan, as described in section 6.8.1.6 Supplier Enablement Plan, to prevent rumours or miscommunications;
j) Change resourcing expectations based on project phases and milestones;
k) Project Team health assessments;
l) People readiness assessments tied to each go-live; and
m) Identifying when, for how long, and the type of GC resources that are required for change management.

The Contractor must ensure the Change Management Plan integrates with the Project Plan and Milestone Schedule. The Contractor must also ensure the coordination between change management, Supplier enablement, and training work streams.

6.7.2.1 Change Management Delivery

The Contractor must:

a) Work in collaboration with the GC in executing the Change Management Strategy and Plan.
b) Identify high risk areas and impact, develop mitigation strategies, and recommended mitigation actions and report results to GC;
c) Facilitate workshops to discuss, analyze and validate changes;
d) Conduct organizational readiness assessments and report findings and recommendations;
e) Perform and complete remediation actions based on readiness assessments and report status to GC;
f) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues; and
g) Provide status reports and risk mitigation plans periodically.

6.7.3 Training Plan

The Contractor must provide to the Project Authority a draft Training Plan within 45 business days following Contract Award for review and approval by the Project Authority.

As a minimum, the Training Plan must describe how the Contractor will:

a) Develop its training approach;
b) Support identification of key stakeholders (in conjunction with change management team) and creation of training materials for user acceptance testing in conjunction with technical team;
c) Develop, document and maintain training and knowledge transfer procedures;
d) Develop and deliver training program to instruct GC personnel on the provision of Contractor Services (e.g., “rules of engagement,” requesting Services);
e) Develop, implement and maintain a GC-accessible knowledge database/Portal;
f) Develop and implement knowledge transfer procedures to ensure that more than one individual understands key components of the business and technical environment;
g) Participate in GC-delivered instruction on the business and technical environment;
h) Provide ongoing training materials for service desk personnel on GC business and technical environments as defined by GC;
i) Training requirements assessment by User type. This must address the initial training requirement for the EPS to “go live” and the ongoing training requirement for new Users or refresher training;
j) Training requirements for administration access;
k) Provide training module content that is copyright and royalty free for modification and redistribution by the GC;
l) As a minimum the training plan for Users must include:
    i. scheduled communications based on the User's migration date;
    ii. instructions on locating training resources;
    iii. details on expected User outcomes;
    iv. detailed instructions on each transition approaches including:
    v. tools and resources that will be available;
    vi. how to populate User profiles;
    vii. frequently asked questions; and
    viii. instructions on providing feedback during the transition.
m) As a minimum the training plan for level 2 service desk agents must include:

i. schedule of transition activities;
ii. description of access rights and roles and responsibilities of level 1 service desk agents during the GC migration;
iii. instructions on locating of support material; and
iv. escalation procedures.

n) As a minimum the training plan for Authorized Administrators must include:
i. schedule of transition activities;
ii. description of access rights and roles and responsibilities of GC and GC Administrators during the GC migration;
iii. Instructions on locating of support material.

6.7.4 Training Delivery

The Contractor must perform the following activities which includes thorough technical and User training, effective communication and successful stakeholder participation:

a) Provide and update training material as needed or concurrent with a major release to address new features and release changes. Training materials must comply with the approved Training Plan;
b) Conduct Authorized Administrator training, including 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;
c) Conduct training for Suppliers, including selected virtual or computer-based training (case-by case basis) and reference materials for Suppliers enabled in the EPS;
d) Conduct User training as requested by the GC, including 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;
e) Conduct Train the Trainer training for Users as defined by GC;
f) Provide role-specific training to Project staff prior to each new product version release in order to facilitate full exploitation of all relevant functional features;
g) If requested by GC, inform and train Users about the end-to-end solution that will support their business requirements, and
h) Provide the training environment to reflect updates and upgrades to the production environment. The training environment must include all GC workflows and must interoperate with a GC managed DFMS training environment.

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

6.8 TRANSITION SERVICES

6.8.1 Transition-In Services

6.8.1.1 Transition-In Plan

The Contractor must provide to the Project Authority a Transition-In Plan within 40 business days of Contract Award for review and approval by the Project Authority.

The Transition-In plan must outline how the GC will transition to the EPS and, as a minimum, must include details on:

a) data conversion and migration;
b) training for EPS Project Team on solution capabilities
c) configuration activities;
d) integration and testing activities;
e) connectivity with Back-office systems e.g. DMFS;
f) discovery research and assessment to determine specific requirements for processing various components of the EPS;
g) testing operational solutions;
h) delivering functional capability;
i) enabling clients and User onboarding;
j) onboarding legacy data;
k) developing solution specific guidelines;
l) developing operational procedure documentation; and
m) developing a thorough implementation readiness assessment plan, readiness assessment schedule, rollback strategy, assessment scorecards and identified and defined critical readiness criteria that will drive go and no-go decisions related to overall readiness and preparedness for going live with any new service or IT environment.

The Contractor must work collaboratively with the GC in the development of the Transition-In Plan.

The Contractor's Transition-In Plan must take a milestones-based approach to managing transition-in activities given the size and complexity of the activities required to ensure a smooth transition-in. The approach must divide the EPS into functional components that can be implemented and delivered rapidly.

The Contractor's Transition-In Plan must include a high level assessment of the GC's current state and identify areas of change, including key policies and business process.

6.8.1.2 Transition-In Delivery (or execution)

The Contractor must:

a) Execute the Transition-In Plan;
b) Identify high risk Transition areas and impact, develop mitigation strategies, and recommended mitigation actions and report results to GC;
c) Review and document current state PWGSC and generic GC processes (based on existing business process documentation and by facilitating workshops) and document gaps between current state and the COTS-provided processes;
d) Make suggestions related to the improvement and re-engineering of existing end-to-end GC-wide processes including a proposed business model (or capability model) and a data model;
e) Facilitate workshops to socialize the processes within the COTS solution and discuss and analyze the proposed GC procurement process optimization and re-engineering;
f) Finalize changes and documentation of new business processes required to align to configured environment;
g) Submit to GC for approval the final documentation of new business processes for the new EPS environment;
h) 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;
i) Perform and complete remediation actions based on readiness assessments and report status to GC;
j) 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;
k) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues;
l) Develop a pre-implementation checklist and post-implementation measurable evaluation criteria;
m) Make go/no-go recommendations and prepare an implementation decision document for approval;
n) Complete all post-cutover activities per the project plan ensuring 100% completion of post-cutover activities; and
o) Provide status reports and risk mitigation plans periodically.

The GC may review the Contractor's interim work products which are produced in the normal course of implementing the EPS. 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.

6.8.1.3 Transition Integration and System Testing

The Contractor must:

a) Provide proposed integration, test strategy and plan to verify functional, performance, and reliability requirements;
b) Recommend integration and testing requirements; and
c) Develop, document and maintain integration and testing plan that meets requirements and adheres to defined policies.
d) Conduct all system testing in accordance with the approved testing strategy and plan; and

e) Provide the GC with copies and/or summaries of the test results confirming that all such tests have been passed.

6.8.1.4 User Acceptance Testing (UAT)

The GC will perform UAT on systems modules and integration work, features and functionalities that are the subject of the EPS configurations as defined in the SOW or as requested by GC. Prior to releasing functional components into production, the Contractor must submit each major and minor release for UAT by the GC. Prior to submitting the release for testing, the Contractor must have completed all of the system testing required with respect to the release.

During the UAT period, the Contractor must:

a) Assist the GC in defining User Acceptance Testing (UAT) scenarios and acceptance criteria;
b) Provide GC with a production-like (test) environment to execute UATs
c) Facilitate the collection of User Acceptance Testing results;
d) Analyze the results of the User Acceptance tests as provided by the GC;
e) Implement corrective action based on the UAT results and GC recommendations; and
f) Assess and communicate the overall impact and potential risk to system components prior to implementing Changes.

Upon receiving a release, the GC will promptly perform UAT in accordance with the applicable scenarios and acceptance criteria, and will inform the Contractor of the outcome of such testing. The GC reserves the right to determine the final acceptance criteria for each release.

The GC will give the Contractor written notice of acceptance of a release when, the release has satisfied the Acceptance Criteria. A release will be deemed to be accepted by the GC only upon written notice of acceptance. If the resubmitted release does not conform to the Acceptance Criteria, the GC may require the Contractor, at no added cost to the GC, to continue to correct the deficiencies, and to take whatever action is necessary so that the Deployment Deliverable conforms to the Acceptance Criteria.

When re-submitting a previously rejected deliverable to the Project Authority, 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.

Once EPS is in production, the Contractor must assess the impact of new releases to the SaaS application(s) on users and system operations and must ensure that Canada has sufficient notice and opportunity to test major updates and material changes to the EPS prior to their release into production. The Contractor must take corrective action to mitigate the impact of any release that negatively impacts EPS operations.

The Contractor must submit a document covering the SAAS Release and Upgrade Policy to the GC within 3 months of Contract Award.

6.8.1.5 Program Stabilization and Post-transition

The Contractor must support the GC following the transition in order to help it achieve a steady state, including:

a) Resolve any stabilization/post-cutover issues identified by GC as high priority within 5 calendar days of each cutover;
b) Conduct post-cutover inspection and submit completed post-cutover checklist within 5 business days following each cutover;
c) Resolve any stabilization/post-cutover issues identified by GC as non-high priority within 15 business days of each cutover;
d) Conduct a stabilization assessment within 10 business days following each cutover including analysis and recommendation;
e) Complete all stabilization activities within 30 business days following each cutover;
f) Develop necessary stakeholder communications immediately following each cutover;
g) Collect, analyze and report stakeholder feedback issues, comments and or request;
h) Conduct a post-Transition review within 60 business days of each cutover;
i) Provide a Transition-In Lessons Learned Report for Project Authority approval no later than 90 business days after each go-live date based on all lessons learned from the execution of the Transition-In Implementation Plan;
j) Incorporate lessons learned into subsequent Transition activities (e.g., future cutovers, transitions, transition-out planning, etc.);
k) Develop necessary stakeholder communications during post-Transition and obtain approval from GC; and
l) Collect, analyze and report stakeholder feedback issues, comments and requests.

6.8.1.6 Supplier Enablement Plan

The Contractor must provide to the Project Authority a draft Supplier Enablement Plan within 10 business days following the approval of the Change Management Strategy for review and approval by the Project Authority.

As a minimum, the Supplier Enablement Plan must include:

a) Supplier Enablement “Best-Fit” Strategy and Overall Approach;
b) Supplier Analysis and Breakdown based on how the EPS will enable purchasing (e.g., PunchOut, hosted catalogue, free form) and the maturity of the Supplier’s IT capabilities;
c) Supplier contact list with current contact information and gaps identified (e.g., missing email, phone, or remit to addresses);
d) Supplier Engagement Plan that outlines how we will move each Supplier through:
    i. 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;

ii. 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 must communicate to the Supplier community on changes to how they do business with GC and what needs to be met to reach implementation;

iii. Positive Perception: build and implement strategies and interaction models to engage Suppliers in developing a readiness to change;

iv. 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. This must include Supplier training, reference materials, and who to contact for additional support during enablement; and

v. Adoption: The change has been operational for long enough to evaluate its worth and impact.

e) Alignment of messaging and timelines between the Supplier Enablement Plan and the Change Management and Training plans.

The Contactor must support the GC in executing the Supplier Enablement Plan and preparing associated communication to the Supplier community. The Contractor must support a range of regular and ongoing initiatives that will be employed to monitor and respond to Supplier expectations, feedback and challenges in adopting the EPS.

6.8.1.7 Product and Solution Roadmap

The Contractor must provide to the Project Authority within 15 business days of Contract Award a Product and Solution Roadmap which must include a feature list of the EPS, as well as a mapping of the EPS to the functional requirements defined in *Part 3 Functional Requirements*.

6.8.1.8 Technology Road Map

The Contractor must provide, on an annual basis throughout the Term of the Contract, a Technology Road Map that will identify upcoming product upgrades and new releases over a 2-year period and allow for the alignment of GC business processes with the evolution of the EPS.

The Contractor must allow a representative of the Project Authority to participate, as an active voting member, on existing client or User committees that solicit feedback on ideas for future software development for all application(s) that makes up the EPS. In addition, on an annual basis, the Contractor must solicit the GC for functionality upgrade ideas and provide feedback as to the feasibility and potential timeline for inclusion in the respective Technology Road Map.

6.8.2 On-Going Support Services

6.8.2.1 On-going Support

The Contractor must support effective management of the EPS for the day-to-day operational activities and the production environment in which it operates, including:

a) Providing documented tools and processes to provide the necessary support for its EPS;
b) Providing status reports detailing progress and updates to the ongoing support.

Any identified deficiencies in the software (i.e. bugs, functionality which ceases to work as intended, security vulnerabilities, etc.) must be corrected within a mutually agreeable timeframe. In the event that agreement on a timeframe cannot be reached and Canada is forced to remove the solution from service, the application will be considered unavailable for the purpose of the service standard 6.13.3.1 Application Availability.

6.8.2.2 Releases, Modifications and Updates

The Contractor must submit a document covering the EPS's Release and Upgrade Policy to the GC within 3 months of Contract Award.

Once EPS is in production, the Contractor must assess the impact of new releases to the EPS application(s) on users and system operations and must ensure that Canada has sufficient notice and opportunity to test major **updates** and material changes to the EPS prior to their release into production. The Contractor must provide support for testing activities to the GC when there are releases, modifications or updates to the EPS, including:

a) Maintain software release matrices across development, quality assurance, and production environments and networks;
b) Provide proposed integration and test plan(s);
c) Conduct integration and security testing for all data and networks based on requirements defined in the plan(s) and GC policies and procedures;
d) Evaluate all new and upgraded system components and services for compliance with GC security rules, regulations and procedures;
e) Conduct User Acceptance Testing for all modifications and updates; and
f) Assess and communicate the overall impact and potential risk to system components.

The Contractor must take corrective action to mitigate the impact of any release that negatively impacts EPS operations.

6.8.3 Maintenance:

The Contractor must continuously maintain and upgrade the EPS, including deploying new updates and releases of the commercial-off-the-shelf solution as they become available, for the entire Term of the Contract.

6.8.4 Transition-Out Services

Prior to the fulfillment of the Contract or prior to the termination of the Contract, as applicable, the Contractor must deliver, enable and support the necessary activities related to transitioning the in-scope EPS to the new service provider (either a new Contractor or to an internal GC Department or Agency). This includes, but is not limited to:

a) Migration of all EPS data to the GC's new service including the information necessary to map the existing EPS's data to the GC's new service;

b) Providing the new service provider with the lessons learned, assets and documentation from the original transition services provided within the scope of this present SOW;
c) Performing and supporting 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 (exiting) can be either directly responsible for, or that are dependent on the Contractor's (exiting) support to bring to completion.

6.8.4.1 Transition-Out Strategy

The Contractor must provide to the Project Authority a Transition-Out Strategy within 12 months following Contract Award for review and approval by the Project Authority. The Transition-Out Strategy must outline how the Contractor's EPS is able to successfully transition to either a new Contractor or to an internal GC Department or Agency. As a minimum, the Transition-Out Strategy must include:

a) proposed knowledge transfer approach;
b) records transfer (volumes, formats), including addressing data conversion issues;
c) approach to how information related to data structures, data domains and data-related processes will be transferred;
d) principles of client transaction history and client account detail migration;
e) probable and perceived transition-out Contractor activities;
f) timeframes for stopping and queuing procurement processes to export data in the destination system;
g) 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. 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.

6.8.4.2 Transition-Out Plan

Within 3 months of notification of the GC's intent to transition-out, the Contractor must provide to the Project Authority a draft Transition-Out Plan to transition out any of the EPS to a new service provider (to a new Contractor or to a new GC Department or Agency).

As a minimum, the Transition-Out Plan must include:

a) project management;
b) data conversion and migration support;
c) business change management support;
d) communications and awareness support;
e) documentation and file support;
f) dual service Contractor transition support;
g) Supplier enablement support;

h) operations support; and
i) User support.

6.8.4.3 Transition-Out Assets and Documentation

To support GC in the Transition-Out phase and when requested by GC, the Contractor must provide the following:

a) assets (sole use and shared) and asset registers;
b) asset maintenance history and status;
c) subcontracts and associated subcontractor relationships;
d) software licenses, including specific references to the software owner's requirements (including transfer);
e) status of Third-Party software covering Contractor, version, upgrade status, license and maintenance fees;
f) Supplier's data and other records (including subcontractor agreements that are required to provision the services);
g) configuration information;
h) data stored in Contractor or third Party compute environments — including cloud based environments;
i) all databases containing GC owned data;
j) programs and projects (open and closed ones);
k) knowledge databases;
l) fault databases;
m) General documentation, including, but not limited to:
    i. organization services design and architecture representations;
    ii. software related documentation (e.g. User, Authorized Administrator);
    iii. updated/recent process and procedure documentation;
    iv. workflow and work instruction documentation;
    v. service management logs - change and incident logs;
    vi. risk register;
n) Tactical documentation, including but not limited to:
    i. service-level reports;
    ii. service catalogue;
    iii. service delivery plans;
    iv. incident and change register;
    v. change and project calendar;
    vi. current and scheduled project documents;
    vii. release schedules;
    viii. performance and capacity management planning;
    ix. innovation and service creation plans related to the involved services;
    x. communication plans and all current and scheduled communication documentation (online and offline);
o) Strategic documentation, including:

i. account plans;
ii. strategic relationship plans;
iii. road maps for technology and services; and
iv. enterprise architecture and governance documentation.

6.9 MEETINGS AND REPORTING

6.9.1 Kick-Off Meeting

The Contractor must organize a Kick-Off Meeting with the Project and the Contracting Authorities in the National Capital Region (NCR), within 10 business days from the date of Contract Award.

The purpose of the Kick-Off Meeting, as a minimum will be to:

a) Review the contractual requirements;
b) 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
c) Discuss the Project Implementation Plan that was proposed as part of the Contractor's bid submission.

The Contractor must prepare and submit the minutes of the meeting within 5 business days to the Project Authority for approval. The minutes of the meeting must 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.

6.9.2 Weekly Status Meeting

The Contractor must organize, schedule and conduct status meetings on a weekly basis with the Project Authority in the NCR throughout the Transition. The focus of these meetings must be to update the Project Authority on key aspects of the EPS project, including schedule review and project health.

The Contractor must prepare and submit the minutes of the meeting within 5 business days to the Project Authority for concurrence/approval. The minutes of the meeting must 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.

6.9.3 Monthly Project Progress Report

The Contractor must prepare and present to the Project Authority for review and approval a monthly Project Progress Status Report. This report must contain the following information:

a) Overall project status;
b) Status in relation to the project management plan;
c) Accomplishments for the current period;
d) Critical Path Analysis;
e) Re-Scheduled Milestones;

f) Planned Activities for the next period;
g) Statistical volumetric information;
h) A summary of service level performance;
i) A list and a description of major events;
j) Outstanding/Resolved Risk and Issue statuses; and
k) Client satisfaction survey results.

6.9.4 Organizational Change Management Reporting

The Contractor must provide Organizational change management reporting on a monthly basis to the Project Authority that captures and reports against all aspects of change management.

6.9.5 Strategic Management Semi-Annual Reviews

The Contractor must prepare and present to the Project Authority and GC senior executives on a semi-annual basis, a Semi-Annual Review including presentations of all EPS components. The Semi-Annual Review must include the following:

a) Project status, including status of key problems;
b) Issues that the EPS is currently facing and a proposal on how to address them; and
c) Risk management status.

6.10 MILESTONES

The dates specified herein are target dates which the Contractor is required to achieve. However, the GC recognizes the dates may change following the consultation and planning phases with the Contractor after Contract Award. As such, at the sole discretion of the GC and in consultation with the Contractor, the dates may be adjusted following Contract Award.

6.10.1 Milestone #1 – Operational Planning

The Contractor must complete Milestone #1 within 4 months of Contract Award. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) Preliminary Project Plan as described in section 6.3.1 of the SoW;
b) Project Management Methodology and Plan as described in section 6.3.2 of the SoW;
c) Relationship Management Plan as described in section 6.3.3 of the SoW;
d) Privacy Management Plan as described in section 6.4.1 of the SoW;
e) IT Security Plan as described in section 6.5.2 of the SoW;
f) IT Service Continuity Plan as described in section 6.5.3 of the SoW;
g) Organizational Change Management Strategy as described in section 6.7.1 of the SoW;
h) Change Management Plan as described in section 6.7.2 of the SoW;
i) Product and Solution Roadmap as described in section 6.8.1.7 of the SoW;
j) Training Plan as described in section 6.7.3 of the SoW;
k) Communications Plan as described in section 5.5.1 of the SoW; and

l) Transition-In Plan as described in section 6.8.1.1 of the SoW.

6.10.2 Milestone #2 – Solution Environment

The Contractor must complete Milestone #2 within 4 months of Contract Award. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) The Contractor has delivered the EPS environment, (with the exception of the GETS environment, if applicable) ready for configuration, integration and testing in both official languages; and
b) The Contractor has delivered the elements of the Project Management Plan, Organizational Change Management Strategy, Change Management Plan, Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the delivery of the EPS environment (with the exception of the GETS environment, if applicable).

6.10.3 Milestone #3 – Supplier Enablement

The Contractor must complete Milestone #3 within 12 months of Contract Award. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) The functionalities described in Section 3.2 General Requirements (excluding section A-08.05), Section 3.2.1 WorkflowRequirements, Section 3.3.3 Portal Requirements (excluding section B-5.00), Section 3.9 Supplier Relationship Management, Section 3.10 Data and Information Management, and Section 3.11 User Management have been, in accordance with the Statement of Work, configured, tested, completed the SA&A process for the release, deployed into production in both official languages, and piloted;
b) The Contractor has delivered the Supplier Enablement Plan;
c) The Contractor has delivered the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the delivery of the functionalities described in Section 3.2 General Requirements, Section 3.2.1 Workflow Requirements, Section 3.3.3 Portal Requirements (excluding section B-5.00), *Section 3.9 Supplier Relationship Management, Section 3.10 Data and Information Management,* and *Section.3.11 User Management*; and
d) The Contractor has delivered the work and objectives described in Part 5 Non-Functional Requirements.

6.10.4 Milestone #4 – Contract Management

The Contractor must complete Milestone #4 within 18 months of Contract Award. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) The functionalities described in Section *3.2.2 Workload Requirement, 3.4 Sourcing and Contract Management, and 3.8 Business Intelligence* have been, in accordance with the Statement of Work, configured, tested, completed the SA&A process for the release, deployed into production in both official languages, and piloted;
b) The Contractor has delivered the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan, Training Plan, Training

Delivery, Transition-In Plan and the Transition-In Delivery applicable to the delivery of the functionalities described in *Section 3.2.2 Workload Requirements*, *3.4 Sourcing and Contract Management, and 3.8 Business Intelligence*; and

c) 100 Contracts (excluding Orders and call-ups) have been sourced and awarded using the EPS.

6.10.5 Milestone #5 – Procurement Management for the GC

The Contractor must complete Milestone #5 within 18 months of Contract Award. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) The functionalities described in section *3.5 Procurement Management* and section *A-08.05* of section *3.2 GeneralRequirements* have been, in accordance with the Statement of Work, configured, tested, completed the SA&A process for the release, deployed into production in both official languages, and piloted;

b) The Contractor has delivered the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan, Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the delivery within PWGSC of the functionalities described in S*ection 3.5 Procurement Management*;

c) EPS is interoperating with PWGSC's DFMS; and

d) 100 Orders have been processed by Users using the EPS.

6.10.6 Milestone #6 – Service Procurement Management for the GC

The Contractor must complete Milestone #6 within 24 months of Contract Award. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) The functionality described in Section 3.6 Service Procurement Management has been, in accordance with the Statement of Work, configured, tested, completed the SA&A process for the release, deployed into production in both official languages, and piloted;

b) The Contractor has delivered the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan, Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the delivery within PWGSC of the functionalities described in Section 3.6 Service Procurement Management; and

c) SOW Based Services Procurement Contracts / Orders have been awarded using the EPS.

6.10.7 Milestone #7 – Fully Operational Baseline

The Contractor must complete Milestone #7 within 24 months of Contract Award. This milestone is considered to be achieved when the Acquisitions Program (Acquisitions Branch and the 5 PWGSC Regional offices) of PWGSC and the Finance and Administration Branch (FAB) of PWGSC have been fully transitioned onto the functionality and the Contractor has delivered all the Work described in the SOW, with the exception of Transition-Out Services as defined in section 6.8.3 Transition-Out Services, the Work described in Part 7.0 Optional Services, the Work described in Milestone #8 – GETS, and the Contractor has submitted

a report substantiating that the Work, inclusive of the report, has been complete, and the Work has been accepted by the Project Authority.

6.10.8 Milestone #8 – Government Electronic Tendering Service (GETS)

The Contractor must complete Milestone #8 within 48 months of Contract Award. Canada will use the first 12 months following Contract Award to design, in consultation with the Contractor, the deployment approach of the work pertaining to this milestone. This milestone will be considered to be achieved when the following work is accepted by the Project Authority:

a) The functionalities described in Section 3.3.2 Government Electronic Tendering Service and section B-5.00 in Section 3.3.3 Portal Requirements have been, in accordance with the Statement of Work, configured, tested, completed the SA&A process for the release, deployed into production in both official languages, and piloted;

b) The Contractor has delivered the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan, Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the delivery of the functionalities described in Section 3.3.2 Government Electronic Tendering Service and section B-5.00 in Section 3.3.3 Portal Requirements;

c) All GC departments and agencies have been on boarded onto the new GETS;

d) All public GC tender notices are being posted and managed using the new GETS; and

e) The Contractor has submitted a report substantiating that the Work, inclusive of the report, has been complete, and the Work has been accepted by the Project Authority.

6.11 DELIVERABLE SUMMARY

Table 20 - Deliverable Summary

SOW Identifier	Deliverable Title
Part 5 Section 5.5.1	Communications Plan
Part 6 Section 6.3.1	Preliminary Project Plan
Part 6 Section 6.3.2	Project Management Methodology and Plan
Part 6 Section 6.3.3	Relationship Management Plan
Part 6 Section 6.4.1	Privacy Management Plan
Part 6 Section 6.4.3	Privacy Impact Assessment
Part 6 Section 6.5.2	IT Security Plan
Part 6 Section 6.5.3	IT Service Continuity Plan
Part 6 Section 6.5.4	Technical Deployment Model
Part 6 Section 6.5.5	Technical Architecture Diagrams
Part 6 Section 6.6	SA&A
Part 6 Section 6.7.1	Organizational Change Management Strategy
Part 6 Section 6.7.2	Change Management Plan

SOW Identifier	Deliverable Title
Part 6 Section 6.7.3	Training Plan
Part 6 Section 6.8.1.1	Transition-In Plan
Part 6 Section 6.8.1.6	Supplier Enablement Plan
Part 6 Section 6.8.1.7	Product and Solution Roadmap
Part 6 Section 6.8.1.8	Technology Roadmap
Part 6 Section 6.8.3.1	Transition-Out Strategy
Part 6 Section 6.8.3.2	Transition-Out Plan

6.12 DELIVERABLES ACCEPTANCE FRAMEWORK

6.12.1 Deliverable Acceptance Framework

With the exception of the deployment of the functional and non-functional requirements described in Part 3 Functional Requirements and Part 5 Non-Functional Requirements, the GC will use the following Deliverables Acceptance Framework for all of the Contractor's deliverables:

a. Deliverables received by the GC will be considered draft until accepted by the GC. If not accepted by the GC, the GC will provide its feedback on the deliverable to the Contractor within 10 business days following receipt;
b. Upon receipt of this feedback by the Contractor, the Contractor and the GC may agree to jointly review the feedback prior to its incorporation into the Final Deliverable;
c. The Contractor must submit the revised deliverable to the Project Authority within 10 business days of the receipt of the GC's feedback, or the joint review of the feedback, whichever is later.
d. The Contractor and the GC may mutually agree to different timelines or an alternate process for given deliverable(s) than the prescribed above.

6.12.2 Acceptance or Rejection of Deliverables

The GC reserves the right to reject deliverables. At the end of the review period as identified in 6.12.1 the Project Authority 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.

6.12.3 Re-submission of a Rejected Deliverable

When re-submitting a previously rejected deliverable to the GC, 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. The Contractor must identify any changes or issues that were not addressed and provide rationale as to why these changes were not included.

6.12.4 Deliverable Submission Process

In order to avoid acceptance delays, inconsistences and contradictions in related Deliverables, the Contractor should take measures to avoid submitting deliverables at the same time, unless stipulated in the Contract. If the Contractor submits multiple deliverables at the same time, outside the stipulated deliverable dates in the Contract, the GC reserves the right for additional review time and will adjust 6.12.1 accordingly.

6.13 SERVICE LEVELS REQUIREMENTS

6.13.1 Performance Measurement and Reporting

The Contractor must provide a Performance Report to the Project Authority on an as-and-when-requested basis containing statistical information on the performance of the EPS as compared to the requirements set out in *Section 6.13 Service Level Requirements*.

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.

6.13.2 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 in the Performance Report, the Contractor must identify any discrepancies, including:

a) Notify the Project Authority as soon as the Contractor becomes aware of such failure;
b) Carry out a root cause analysis to investigate the underlying cause of the failure and preserve any data indicating the cause of the failure;
c) Take action as agreed with the Project Authority to minimize the impact of the failure and prevent it from recurring;
d) If practical, correct the failure immediately in order to resume fulfillment of the Service to the applicable Service Standard;
e) 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;

f) Advise the Project Authority of the status of all remedial efforts being undertaken by the Contractor with respect to the underlying cause of the failure; and

g) In calculating the Contractor's compliance with the Service Standards, any performance issues:

i. caused by factors outside of the Contractor's control;

ii. that resulted from any actions or inactions of GC or any third parties not within the Contractor's control;
or

iii. that resulted from GC's equipment and/or third party equipment not within the primary control of the Contractor must not be included in such calculations (unless the event is the result of acts or omissions of the Contractor).

At the GC's request, the Contractor must provide substantiation that the cause of the service issue is reasonably outside of its control. The Contractor must review Section 7.10.9 Service Level Failure and Earn Backs of Part 7 – Resulting Contract Clauses

6.13.3 Service Standards

6.13.3.1 Application Availability

This service level measures the availability of the EPS.

Table 21 - Application Availability

APPLICATION AVAILABILITY		
Service Measure	Performance Target	SLR Performance %
Percentage	The percentage of time that the application is available for normal business operations. (06:00 to 24:00 EST, 7 days a week)	Production Applications: 99.5%
Formula	[Number of minutes during the month being report on when the production applications and their various components were operating without any Priority Level One or Two incidents within the control of the Contractor] divided by [Total number of minutes during such month minus (number of minutes 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 either uptime or downtime data.	

6.13.3.1.1 Contractor Service Level Failure Credits

Application Availability Production Applications	Service Level Failure Credits
Less than 99.5% but equal to or greater than 97.0%	2% Credit
Less than 97% but equal to or greater than 95.0%	5% Credit
Less than 95%	10% Credit

6.13.3.2 Reporting

This service level identifies the adherence of the Contractor to the agreed schedule and accuracy of reports, as identified in the SOW.

Table 22 - Reporting

REPORTING		
Service Measure	**Performance Target**	**SLR Performance %**
Reporting Schedule	Provision of reports, as identified in the SOW, within the defined time lines in of the Contract	95%
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 by GC in consultation with the Contractor after Contract Award	

6.13.3.2.1 Contractor Service Level Failure Credits

Reporting Schedule	Service Level Failure Credits
Less than 95% but equal to or greater than 90%	2% Credit
Less than 90% but equal to or greater than 85%	5% Credit
Less than 85%	10% Credit

6.13.3.3 EPS Service Desk Availability

Table 23 - Service Desk Availability

SERVICE DESK AVAILABILITY		
Service Measure	Performance Target	SLR Performance %
Schedule	Tier 1 & Tier 2 Mon- Fri, 07:00-19 :00 Tier 3 Mon-Fri, 09:00-17:00	99%
Formula	Availability (%) = 100% - Unavailability (%) where Unavailability is defined as: (Σ Outage Duration × 100%) ÷ (Schedule Time - Planned Outage)	
Measurement Interval	First month: Measure daily Thereafter: Measure daily	

SERVICE DESK AVAILABILITY	
Reporting Period	First month: Report weekly Thereafter: Report monthly
Measurement Method/Source Data	TBD by GC in consultation with the Contractor after Contract Award

6.13.3.3.1 Contractor Service Level Failure Credits

Service Desk Availability	Service Level Failure Credits
Less than 99% but equal to or greater than 97.0%	2% Credit
Less than 97% but equal to or greater than 95.0%	5% Credit
Less than 95%	10% Credit

6.13.3.4 EPS Service Desk Incident Acceptance Response Time

Incident Acceptance Response Time is the measure of 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 Contractor to the time it is logged and assigned for resolution in the service desk application.

Table 24 - Incident Acceptance Response Time

INCIDENT ACCEPTANCE RESPONSE TIME		
Service Measure	Performance Target	SLR Performance %
Percentage	Priority 1 Incident: ≤ 60 elapsed minutes Priority 2 Incident: ≤ 60 elapsed minutes Priority 3 Incident: ≤ 2 Standard Operating Hours Priority 4 Incident: ≤ 4 Standard Operating Hours	≥ 95% (all Priority Levels)
Formula	[Number of Incidents (of all Priority 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 Priority Levels) received and accepted during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”	
Measurement Interval	Monthly	
Reporting Period	Monthly	
Measurement Method/Source Data	TBD by GC in consultation with the Contractor after Contract Award	

6.13.3.4.1 Contractor Service Level Failure Credits

Incident Acceptance Response Time	Service Level Failure Credits
Less than 95% but equal to or greater than 93.0%	2% Credit
Less than 93% but equal to or greater than 90.0%	5% Credit
Less than 90%	10% Credit

PART 7: OPTIONAL SERVICES

7.1 OPTIONAL PROFESSIONAL SERVICES

The Work described in this section will be requested by GC through a Task Authorization on an as and when requested basis.

7.1.1 Procurement Advisory Services

The Contractor must provide Procurement Advisory Services on an as and when requested basis. The Contractor must propose resources that are qualified and have experience providing Procurement Advisory Services for the provision of the services and their applicable All Inclusive Daily Fixed Rates as per *Annex 3 – Price Schedule*. Procurement Advisory Services may include, but are not limited to, advisory on:

a) Spend Optimization & Category opportunity identification
b) Complex sourcing and contracting
c) Supplier relationship and risk management
d) Strategic sourcing
e) Procurement Policy Development
f) Technology enablement

7.1.2 Additional Change Management and Business Transition Support Services

In addition to the services described in *Section 6.8 Transition Services*, the Contractor must, on an as and when requested basis, provide additional services and must propose resources that are qualified and have experience providing Additional Change Management and Business Transition Support Services for the provision of the services and their applicable All Inclusive Daily Fixed Rates as per *Annex 3 – Price Schedule*. Additional Change Management and Business Transition Support Services may include, but are not limited to:

a) Procurement Process Optimization and Re-engineering
b) Organizational Change Management
c) Development of Customized Training
d) SAP System Architecture and Configuration
e) Master data Architecture

7.1.3 Professional Services Categories

For Work described in accordance with *Section 7.1.1 Procurement Advisory Services*, *Section 7.1.2 Additional Change Management and Business Transition Support Services, Section 7.2.1 Additional System Configuration, Section 7.2.2 Legacy Data Migration, Section 7.2.3 Third Party Integration,* and *Section 7.2.5 Access to Data of this annex and Section 1.1 Remediation(s)* of *Annex 2 – Security and Privacy,* the Contractor must provide the professional services outlined below on an as and when 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.

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.

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.

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.

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.

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.

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.

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 trade-off 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.

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.

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.

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.

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.

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.

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.

IT 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 Federal, Provincial or Territorial IT Security policies, System IT Security Assessment and Authorization 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: Business Need for Security, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings
- 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
- Develop and deliver training material relevant to the resource category

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

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

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:
  - Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH
  - TCP/IP, UDP, DNS, SMTP, SNMP
  - Approved GC Cryptographic Algorithms
  - Directory Standards such as X.400, X.500, and SMTP
  - Networking Protocols (e.g., HTTP, FTP, Telnet)
  - Network hardening (for example: shell scripting, service identification)
  - Technical IT Security safeguards
  - IT Security tools and techniques
  - Operating Systems such as MS, Unix, Linux, and Novell
  - Intrusion detection systems and firewalls
  - Network routers, multiplexers and switches
  - 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

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:
  - 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
  - War dialers, password crackers
  - Public Domain IT vulnerability advisory services
  - Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap

- Networking Protocols (HTTP, FTP, Telnet)
- Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP
- Wireless Security
- Intrusion detection systems, firewalls and content checkers
- 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

The Work described in this section will be requested by Canada through a Task Authorization on an as and when requested basis.

7.2.1 Additional System Configuration

In accordance with Part 5 Non-Functional Requirements, GC anticipates the need to modify the solution 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.

The Contractor must provide additional services and must propose resources that are qualified and have experience providing Additional System Configuration for the provision of the services and their applicable All Inclusive Daily Fixed Rates as per *Annex 3 – Price Schedule*.

Once EPS is operational, the Contractor must provide Additional System Configuration services, on an as and when 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:

a) Workflows;
b) Reports;
c) Templates and Forms;
d) System Fields; and
e) Localization and Branding.

7.2.2 Legacy Data Migration

The Contractor must provide Legacy Data Migration services and must propose resources that are qualified and have experience providing Legacy Data Migration for the provision of the services and their applicable All Inclusive Daily Fixed Rates as per *Annex 3 – Price Schedule*.

In accordance with *Section 4.4 EPS Technology Requirements*, the Contractor must deliver, enable and support data migration from existing GC legacy systems and transitional data feeds not already articulated in the Statement of Work, on an as and when requested basis.

7.2.3 Third Party Integration

The Contractor must provide Third Party Integration and must propose resources that are qualified and have experience providing Third Party Integration for the provision of the services and their applicable All Inclusive Daily Fixed Rates as per *Annex 3 – Price Schedule*.

In accordance with *Part 4 Technical Requirements*, 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.

7.2.4 Tender Feeds

In accordance with *Section 3.3 Portal Requirements*, 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.

7.2.5 Access to Data

On an as requested basis, the Contractor must provide a copy of GC's EPS data in a manner to be defined by the GC. The copy of data will reside in Canada. Requirements such as types of data, security requirements, file format, frequency of delta updates and the location of data storage will be determined at a later date.

7.2.6 Functional Requirements: SECTION F – FINANCIAL MANAGEMENT

The Contractor must, on an as and when requested basis for each instance:

a) configure;
b) test;
c) complete the SA&A process for the release;
d) pilot and deploy the functionalities listed in Table 9 – Financial Management Requirements to the portfolio of departments associated with a DFMS instance as described in the table of section 1.3 Volumetric Data, sub-section k) Departmental Financial Management System (DFMS) Instances;
e) deliver, enable and support the interoperability of the functionalities listed in Table 9 – Financial Management Requirements with the DFMS instance;
f) deliver the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the deployment of the functionalities listed in Table 9 – Financial Management Requirements to a department; and
g) ensure the portfolio of departments associated with the DFMS instance has been fully transitioned onto the functionalities listed in Table 9 – Financial Management Requirements.

7.2.6.1 Objectives

The overall objective of this section is to describe the requirements for the financial management functionalities within the EPS, including goods receipt and invoice management.

7.2.6.2 General

The General subsection describes the functionalities that the Contractor must provide to permit specific Users to view, accept, and reject invoices and goods receipts, and provide Users the flexibility to add comments and attachments electronically.

7.2.6.3 Goods Receipt Management

The Goods Receipt Management subsection describe the functionalities that the Contractor must provide to allow for the configurability of partial and multiple receipts of Goods and Services to be handled within the EPS.

7.2.6.4 Invoice Management

The Invoice Management subsection includes requirements that the Contractor must provide with regards to 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.

7.2.6.5 Requirements

Table 9 - 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	Deleted
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. dispatch 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 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 EPS and connect to the applicable Order (e.g. warehouse loading dock receipt process).
F-01.10	to load ERP non-catalogue spend data on an as and when required basis.
F-02.00	**Goods Receipt Management** 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.
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 DFMS (e.g. goods received, damaged).
F-02.04	Deleted
F-03.00	**Invoice Management** 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.

SOW NUM	Requirement
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	Deleted
F-03.06	to allow Suppliers to submit invoices and credit memos in multiple currencies in at least the following methods: i. Manual input: Data is inputted into a standard form with required and optional fields. ii. Uploaded file: Data are uploaded in a structured file format (e.g. XML, UBL). iii. 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 assign a unique identifier to each invoice and link to the appropriate order.
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 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).
F-03.15	to send line level invoice and goods receipt information to the DFMS in order to initiate the payment.

7.2.7 Government Wide Deployment – DFMS Instance Transition-In

On an as and when requested basis for each instance, the Contractor must,

a) configure;
b) test;
c) complete the SA&A process for the release;
d) pilot and deploy EPS to the portfolio of departments associated with a DFMS instance as described in the table of section 1.3 Volumetric Data, sub-section k) Departmental Financial Management System (DFMS) Instances;
e) deliver, enable and support the interoperability of EPS with the DFMS instance;

f) deliver the elements of the project management plan, Organizational Change Management Strategy, Supplier Enablement Plan, Change Management Plan Training Plan, Training Delivery, Transition-In Plan and the Transition-In Delivery applicable to the full deployment of the EPS to a department; and
g) ensure the portfolio of departments associated with the DFMS instance has been fully transitioned onto the EPS.

7.2.8 Government Wide Deployment – DFMS Instance Operational

For the applicable DFMS instance requested, the above elements in 7.2.7 must be completed within twelve months of Canada's request. Canada may request deployment of more than one DFMS instance to be in the same request and Canada may request deployment of some instances at later dates during the period of the Contract.

7.3 OPTIONS FOR OTHER CANADIAN BROADER PUBLIC SECTORS

7.3.1 Extending Access to Other Canadian Broader Public Sectors

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 Broader Public Sectors to acquire a EPS

On an as requested basis, the Contractor agrees to extend the provision of the EPS as defined in the Contract to any government of any province or municipality in Canada, any Canadian aid agency or public health organization or any intergovernmental organization with substantially the same terms and conditions of this Contract.

ANNEX 2

SECURITY AND PRIVACY

Table of Contents

1. SECURITY AND PRIVACY

This annex provides the security requirements that the e-Procurement Solution (EPS) will be required to implement. Following Contract Award, the Public Works and Government Services Canada (PWGSC) Security Assessment and Authorization (SA&A) process, as described in *section 6.6 PWGSC Security Assessment Authorization (SA&A) Process* of Annex 1 – Statement of Work, will assess how these requirements are addressed by the Contractor to assess compliance with Canada's security requirement.

If at any point during the SA&A process the Contractor cannot meet the security requirements described in *Section I – Security Requirements* to Canada's satisfaction, or if the security risks discovered through the SA&A process are deemed unacceptable by Canada, Canada, at its own discretion, may exercise any rights or remedies to which it is entitled under the Contract (including the right to terminate the Contract for default).

The GC has identified security controls to meet the Business IT Security Profile. The implementation of this set of controls by the Contractor must ensure GC information within the EPS is properly safeguarded to maintain a level of residual risk that is acceptable to Canada. Where Canada agrees, some of the security controls identified in *Section I – Security Requirements* below may be satisfied through existing industry standards, certifications and best practices.

As part of the SA&A process, if the security requirement are not met, corrective actions will be requested by Canada to address the concern. Canada may decide in its sole discretion whether it is satisfied that the remediation is adequate.

1.1 REMEDIATION(S)

Controls that are assessed as non-compliant during the SA&A process will be assessed by the Canada for risk exposure to the GC information. For risk item(s) that are assessed as unacceptable by Canada through the SA&A process, the Contractor must put in place adequate remediation to mitigate the risk(s) associated with the EPS.

1.2 OVERVIEW

This document consists of two sections:

1. Section I is a listing of the security requirements which have been categorized by the control families in Communications Security Establishment (CSE) Information Technology Security Guidance (ITSG)-33 (refer to https://www.cse-cst.gc.ca/en/node/265/html/22814 for more details on ITSG-33), as well as to the Government of Canada (GC) departmental and industry best practices. Throughout the life of the EPS, evidence of meeting the requirements will be assessed through the SA&A process.

2. Section II is a sample Security Requirements Traceability Matrix.

1.3 EPS IT SECURITY FOR SOFTWARE AS A SERVICE

The GC is moving to align with industry in adopting standards and best practices for sharing information. To assist in this initiative, the CSE has developed *The IT Security Risk Management: A Lifecycle Approach (as detailed within the CSE ITSG-33),* which provides the tools and guidance for GC organizations and contractors working on behalf of GC to ensure the risks to GC information systems are:

- identified;
- reported; and
- mitigated throughout a System Life Cycle (SLC).

Throughout the Term of this Contract, the need to protect GC information is of utmost importance and will be the driving force in determining the best method for securing the information assets.

The Business Needs for Security defines the business's targets for security, which are used to select the applicable controls from the CSE's ITSG-33 control catalogue based on the sensitivity, integrity and availability of the information.

1.4 SECURITY ASSESMENT AND AUTHORIZATION GATES

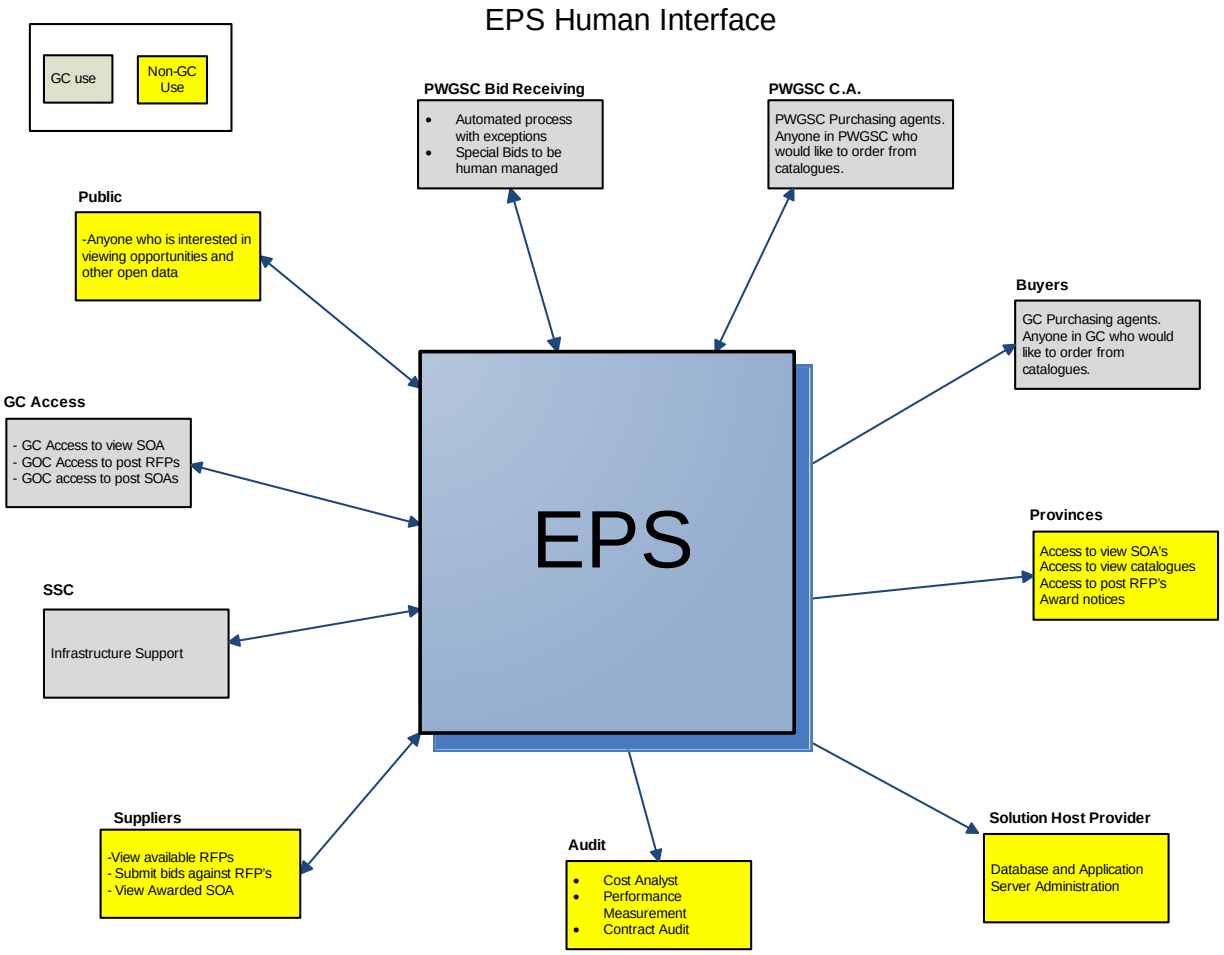
The SA&A process is based on secure System Development Lifecycle (SDLC). For the EPS, GC has identified three SA&A gates to ensure that the EPS is being designed, built, and integrated with security safeguards incorporated, thus providing a secure and stable EPS for GC. This is an iterative approach to the migration of the EPS from design and development to operational status. GC has outlined a set of deliverables expected at each gate. These deliverables will be reviewed and assessed, by GC, for compliance with the requirements identified in *Section I* of this annex. Furthermore, understanding that all areas of the SaaS may not be visible to GC, the Contractor must provide any Service Level Agreements (SLAs) or Memorandums of Understanding (MOUs) that may be in place, for GC's review, to facilitate a better understanding of the security posture of the EPS.

The Contractor must identify any industry standards or certifications they are compliant to in support of its EPS. The SAS 70 standard is one such standard which includes operating procedures for physical and perimeter security of data centers and service providers. Access, storage, and processing of sensitive data must be carefully controlled and is governed under standards such as ISO-27001, Sarbanes-Oxley Act [SOX], Gramm-Leach-Bliley Act [GLBA], Health Insurance Portability and Accountability Act [HIPAA] and industry standards like Payment Card Industry Data Security Standard [PCI-DSS].

1.5 BUSINESS CONTEXT

1.5.1 Business Use Cases

Figure 1 below provides an overview of the business use cases for the human interfaces associated with the EPS. It illustrates diversity of the user base for the EPS.



1.6 TECHNICAL CONTEXT SUMMARY

The EPS must be 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 Technology Requirements for the EPS are defined in *Section 4.4 EPS Technology Requirements* of Annex 1 – Statement of Work.

The EPS must be hosted as a cloud-based solution and the Contractor must ensure data segregation of the GC's data. 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)

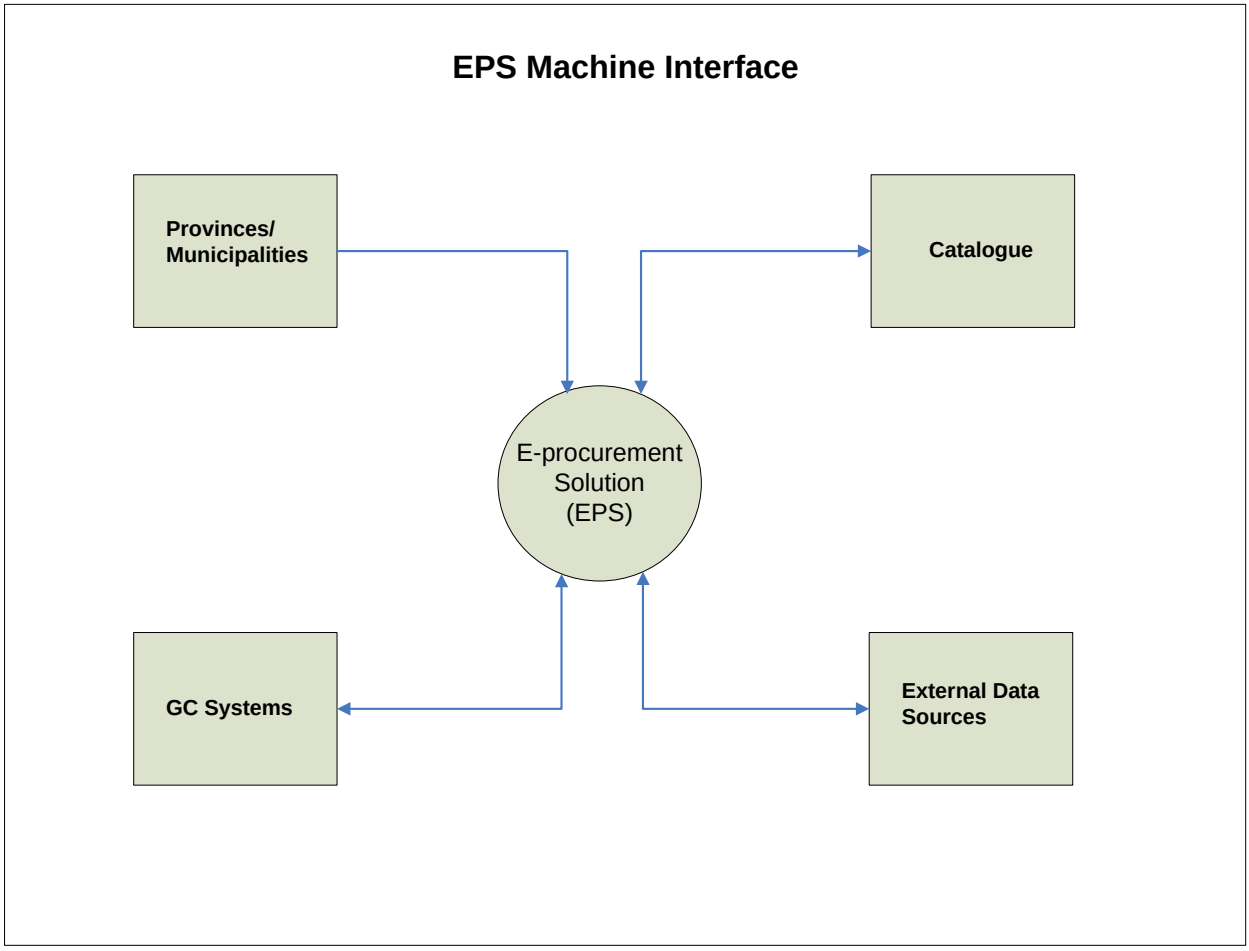
process. While the overall P2P initiative is still in the planning stage, the EPS needs to be part of the overall business flow to support P2P.

The EPS must interoperate, through the Enterprise Service Bus (ESB) with the multiple GC installations of the SAP Department Financial and Materiel Management System (DFMS). The primary 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 4.3 Interfaces with Government of Canada Systems* of Annex 1 – Statement of Work.

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 4.5 Secure Access* of Annex 1 – Statement of Work provides more information on Secure Access requirements.

1.6.1 Machine Interface

Figure 2 below provides an overview of the machine interface associated with the EPS.



1.7 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 and data.

1.7.1 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.

1.7.2 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.

1.7.3 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.

SECTION I - SECURITY REQUIREMENTS

Table 1 below details the EPS security requirements.

EPS RFP ID	Requirement Category	Description
E2.1	Access Control	The Contractor must a) develop, disseminate, and review/update annually, the access control policies and associated access control requirements for EPS components; and b) provide GC 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 EPS User Accounts and Generic Accounts, as follows: a) assign a unique EPS Account and Display Name in accordance with the standard defined in SOW, 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 GC; and e) return the assigned EPS Account, Display Name, and one-time password to the Account Requester.
E2.3	Access Control	The Identity Credential and Access Management Service must a) prevent the re-use of an EPS Account as specified by GC; b) allow Account suspension policies as specified by GC; c) not allow access to a suspended Account; d) not allow an Account to send and receive EPS work flow messages if the Account is suspended; and e) not allow direct access to the EPS Solution Service for any Account, as specified by GC.
E2.4	Access Control	The Contractor must manage EPS 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 EPS 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 EPS Operators are terminated, transferred, or EPS 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 GC, and iv) temporary and emergency accounts over a given age; l) granting access to the e-Procurement Service based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by the Contractor or GC; 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.
E2.5	Access Control	The EPS 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 EPS accounts of which the User is not the primary owner.
E2.6	Access Control	The EPS must enforce access authorizations for Operators.
E2.7	Access Control	The EPS Data Loss Prevention (DLP) capability must a) detect violations of data loss prevention policies and apply response actions 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 in writing between the Contractor and GC; b) allow real-time enforcement of data loss prevention policies based on the contents of the EPS transaction attributes including but not limited to i) strings, string patterns, and keywords within the transaction body; ii) file type of any attachments; and iii) specific domain(s) such as those known for malicious content.
E2.8	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.

E2.9	Access Control	The Contractor must implement a least privileges policy for EPS 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 EPS.
E2.10	Access Control	The EPS must: 1. Display a logon banner approved by GC on the login page of any web-based application for Users. 2. include an access control mechanism that: a) prevents access to EPS components or resources without identification, authentication, and authorization; b) displays a GC-approved logon warning banner that authorized operators must acknowledge prior to being granted access to EPS 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 EPS components. e) include an operator session lock mechanism that: i. prevents further access to components by automatically initiating an operator session lock after a period of inactivity no longer than 60 minutes; ii. prevents further access to components by initiating an operator session lock when requested by the operators; iii. 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 iv. unlocks an operator session after successful authentication of the operator.
E2.11	Access Control	The Contractor must ensure that any use of Remote Management within the EPS take place using a method approved by Canada that includes: a) Remote Management must be restricted to EPS located within a contractor Service Delivery Point using EPS 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 EPS 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.

E2.12	Access Control	The Contractor must establish Policies and procedures, supporting business processes and technical measures, implemented within any environments supporting the EPS in order to protect EPS from 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 in compliance with CSE ITSB-111 for Protected 'B' data c) Security hardening by replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) d) User access including Operators to wireless network devices restricted to authorized personnel e) The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network.
E2.13	Access Control	The Contractor must implement a mobile device policy for EPS that includes the following at minimum a) Anti-malware awareness training, specific to mobile devices, must be included in the contractor's information security awareness training; b) A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data; c) The contractor must have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store. d) If Applicable, the Bring Your Own Device (BYOD) policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage. e) The contractor must have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The contractor must post and communicate the policy and requirements through the company's security awareness and training program. f) All cloud-based services used by the Contractor's mobile devices or BYOD must be pre-approved for usage and the storage of eProcurement Solution GC business data. g) The contractor must have a documented application validation process to test for mobile device, operating system, and application compatibility issues. h) The BYOD policy must define the device and eligibility requirements to allow for BYOD usage. i) Contractor must keep and maintain an inventory of all mobile devices used by the Contractor to store and access e- Procurement Solution GC data. j) Contractor must include for each device in the inventory details of all changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)). k) A centralized, mobile device management solution must be deployed to all mobile devices permitted to store, transmit, or process customer data.

		l) The mobile device policy must require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and must be enforced through technology controls. m) The mobile device policy must prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and must enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management). n) The BYOD policy, if applicable, must include clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy must clearly state the expectations regarding the loss of non GC eProcurement Solution business data in the case a wipe of the device is required. o) BYOD or contractor-owned devices are configured to require an automatic lockout screen, and the requirement must be enforced through technical controls. p) Changes to mobile device operating systems, patch levels, or applications must be managed through the contractor's change management processes. q) Password policies, applicable to mobile devices, must be documented and enforced through technical controls on all contractor devices or devices approved for BYOD usage, and must prohibit the changing of password/PIN lengths and authentication requirements. r) The mobile device policy must require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported). s) All mobile devices permitted for use through the contractor's BYOD program or a company-assigned mobile device must allow for remote wipe by the contractor's corporate IT or must have all company-provided data wiped by the contractor's corporate IT. t) Mobile devices connecting to contractor networks, or storing and accessing company information, must allow for remote software version/patch validation. u) All mobile devices must have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel must be able to perform these updates remotely. v) The BYOD policy must clarify the systems and servers allowed for use or access on a BYOD-enabled device.
E2.14	Access Control	DELETED
E2.15	Access Control	The Contractor must limit the use of Contractor-controlled portable storage media within the EPS (e.g., thumb drive) as follows: a) restrict the use to authorized Operators only, and b) restrict the use to EPS components only.
E2.16	Security Awareness and Training	The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for awareness and training.

E2.17	Security Awareness and Training	The Contractor must provide security awareness and training for EPS Operators as follows: a) as part of initial training for new Operators; b) before authorizing access to the EPS or performing assigned duties, and c) annually or when security impacting changes to the EPS occur.
E2.18	Security Awareness and Training	The Contractor must monitor and document EPS security awareness and training for EPS Operators including: a) documenting who received what training course and when, and b) retaining records for the last three (3) years.
E2.19	Audit and Accountability	The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for audit and accountability.
E2.20	Audit and Accountability	The EPS 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.
E2.21	Audit and Accountability	The Contractor must a) review and update the list of auditable events for EPS at minimum once in 180 Business Days; b) include execution of privileged functions in the list of audit events; c) log events such as database logs, application logs, firewall logs, etc. to allow Canada to identify and assess potential issues; and d) automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.
E2.22	Audit and Accountability	The Contractor must ensure that the EPS: a) audits events such as unauthorized access to the EPS, unauthorized modification, changes to security attributes, privileged access to data fields, and b) produces audit records that contain sufficient information 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 or audit events identified by type, location, or subject; and manages the content of audit records that are generated.
E2.23	Audit and Accountability	The Contractor must perform capacity management on the EPS audit record storage by: a) allocating enough audit record storage capacity; b) configuring auditing to prevent storage capacity being exceeded;

		c) alerting the Contractor's Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and d) overwriting the oldest audit records if storage reached maximum capacity.
E2.24	Audit and Accountability	The EPS 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.
E2.25	Audit and Accountability	The EPS must use internal system clocks that are synchronized with an authoritative time source, approved by GC, to generate time stamps for audit records.
E2.26	Audit and Accountability	The EPS 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 GC.
E2.27	Security Assessment and Authorization	The Contractor must develop an EPS vulnerability mitigation plan, for approval by Canada, within five (5) Business Days of completion of a vulnerability assessment. The plan must include proposed protection measures to mitigate the risks identified from the vulnerability assessment.
E2.28	Configuration Management	The Contractor must develop, document, and maintain under configuration control, a current baseline configuration (N) of the EPS and the previous version (N-1).
E2.29	Configuration Management	The Contractor must only allow software authorized by the Contractor to execute on the EPS. The software authorization process must be documented by the Contractor.
E2.30	Configuration Management	The Contractor must a) plan, test the implementation of new and changed software, hardware and documentation for an EPS release not using the production environment or the Control Test Environment of the EPS; b) implement new and changed software, hardware and documentation for an EPS release as approved by Canada; and c) develop and implement procedures for the distribution, installation, and rollback of changes implemented for an EPS release.
E2.31	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 GC 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.

E2.32	Configuration Management	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.
E2.33	Configuration Management	The Contractor must review EPS Operator privileges on an annual basis.
E2.34	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.
E2.35	Configuration Management	The Contractor must open a security Incident Ticket when an unauthorized configuration change is detected in the EPS.
E2.36	Configuration Management	The Contractor must configure the EPS to provide only essential capabilities and specifically prohibits or restricts the use of functions, ports, protocols, or services as approved by Canada.
E2.37	Configuration Management	The Contractor must develop, document, and maintain an inventory of the EPS 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 GC; and e) is updated as an integral part of component installations, removals, and EPS updates.

E2.38	Configuration Management	The Contractor must provide an EPS configuration management plan that: a) addresses roles, responsibilities, and configuration management processes and procedures; b) defines the Configuration Items for EPS 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 EPS 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 EPS before installation; III. incorporating flaw remediation into the EPS configuration management process; e) defines the processes for patch management of the EPS 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 GC; 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 GC of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of EPS.
E2.39	Configuration Management	The Contractor must provide GC with a EPS 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 EPS (e.g., a concept of operation); d) method used to uniquely identify configuration items; e) configuration item identification method; and f) means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items.
E2.40	Contingency Planning	The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for contingency planning.
E2.41	Contingency Planning	The Contractor must work in conjunction with GC to establish national restoration priorities for EPS in an order of precedence as specified by GC.

E2.42	Contingency Planning	The Contractor must a) test the backup data for EPS monthly to verify media reliability and data integrity; and b) use a sample of backup data for EPS in the restoration of selected EPS functions as part of service continuity plan testing.
E2.43	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 EPS.
E2.44	Contingency Planning	The Contractor must restore the EPS to a known state after a disruption, compromise, or failure.
E2.45	Identification and Authentication	The Contractor must provide GC with the operational security procedures that includes operational roles and responsibilities for identification and authentication requirements specified in this SOW.
E2.46	Identification and Authentication	The EPS 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 GC; f) allow one-time temporary passwords must be sufficiently random so as to not be predictable as approved by GC; g) allow automatic advanced notification of pending password expiry as specified by GC; h) allow password recovery policies and processes; and i) authenticate all Software Client access to the EPS.
E2.47	Identification and Authentication	The EPS 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 EPS Level 2 credential to access the EPS as a User and use an additional X.509 credential to access the EPS for administrative functions.).
E2.48	Identification and Authentication	The EPS 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.

E2.49	Identification and Authentication	The Contractor must manage EPS 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 EPS 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 EPS Operators are terminated, transferred, or EPS 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 GC, and iv) temporary and emergency accounts over a given age; l) granting access to the EPS based on: i) a valid access authorization; ii) intended system usage, and iii) other attributes as required by The Contractor or GC; 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.
E2.50	Identification and Authentication	The EPS 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 (https://www.cse-cst.gc.ca/en/node/267/html/22784): i) password changes; ii) credential registrations; iii) password recovery; iv) expired credentials
E2.51	Identification and Authentication	DELETED

E2.52	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 EPS 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.
E2.53	Identification and Authentication	The EPS 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.
E2.54	Identification and Authentication	The EPS 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 GC 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.
E2.55	Identification and Authentication	The Contractor must require that the registration process for EPS 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).
E2.56	Identification and Authentication	The EPS must not transmit clear text passwords over any network.

E2.57	Identification and Authentication	The Contractor must not allow unencrypted static authenticators to be embedded in EPS applications or access scripts or stored on function keys.
E2.58	Identification and Authentication	The EPS must obscure feedback of Operator authentication data (e.g., masking password fields) during the authentication process.
E2.59	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 e-Procurement Solution 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.
E2.60	Incident Response	The Contractor must a) provide GC with the operational security procedures that includes operational roles and responsibilities for Incident response requirements specified in this SOW. b) implement and test the service continuity plan (all processes, procedures, roles, responsibilities etc.) on an annual basis, and provide the test results to GC within 10 Federal Government Working Days of completion of the service continuity plan testing. c) provide a service continuity plan (SCP) to GC that includes: i. detailed plan and documented processes for restoring EPS; ii. details the communications plan with GC and its suppliers; iii. details plan and processes for transferring operational, management and administration functionality to a backup operations centre; iv. back up strategies for datacenter facilities, network facilities, operational support systems and data, and key service components; v. how The Contractor will ensure that its suppliers have in place service continuity plans; vi. describes the process for testing the Service Continuity Plan; vii. steps The Contractor will take if any of its key suppliers go out of business, and viii. 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 GC.
E2.61	Incident Response	The Contractor must provide a final version of the Service Continuity Plan within 15 Federal Government Working Days after receiving comments from GC on the draft Service Continuity Plan.
E2.62	Incident Response	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 GC.

E2.63	Incident Response	The Contractor must provide to GC 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 GC's service continuity requirements.
E2.64	Incident Response	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 Canada 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 Canada's sole discretion. Canada will accept certificate of compliance as evidence.
E2.65	Incident Response	The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by GC, 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 GC; 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 GC of the degree of non-compliance.
E2.66	Incident Response	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 GC (e.g. the Canadian Cyber Incident Response Centre (CCIRC) (http://www.publicsafety.gc.ca/prg/em/ccirc/anre-eng.aspx).
E2.67	Incident Response	The Contractor must provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase, with the and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of EPS Security Incidents.
E2.68	Incident Response	The Security Operations Center (SOC) must: a) Coordinate Security Incident response in close coordination with GC; 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 GC representatives for security incidents; d) not impact operations of EPS in case of a Contractor Security Operations Center (SOC) failure; e) notify GC within 15 minutes if Contractor SOC is not available and provide contact name GC can communicate as necessary during The Contractor SOC outage.
E2.69	Incident Response	The SOC must work with GCs Information Protection Centre (IPC) for activities that include: a) integration of processes; b) oversight; c) security Incident handling and response; d) auditing; e) Security Incident containment, eradication and recovery that include:

		i. ability to dispatch the IT Security Incident Recovery Team (ITSIRT) to The Contractor site; and ii. allowing GC to provide on-site guidance and coordination.
E2.70	Incident Response	The Contractor must automatically provide Incident Ticket information by secure e-mail to a pre-defined distribution list for each EPS for Incidents where GC 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).
E2.71	Incident Response	The Contractor must continue to automatically send secure e-mail upon updates of Incidents until the Incident is closed or GC cancels the automatic update reporting for the Incident.
E2.72	Incident Response	The Contractor must implement mitigation measures (e.g., firewall blocks, Intrusion Detection Prevention signatures, removing malicious malware) to contain a Security Incident, protect against cyber threats or address vulnerabilities.
E2.73	Incident Response	The Contractor must provide a Security Incident post-mortem report to GC, within 72 hours of a request by GC, 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 EPS, and j) recommendations to improve EPS.
E2.74	Incident Response	The Contractor must monitor on a continuous basis events on the EPS to: a) detect attacks, Incidents and abnormal events against the EPS; b) identify unauthorized use and access of EPS Data and EPS components, and. c) respond, contain, and recover from threats and attacks against the EPS.
E2.75	Incident Response	The Contractor must provide training for EPS Operators in their security Incident response roles and responsibilities and provide annual refresher training.

E2.76	Incident Response	The Contractor must test the Incident response process for the EPS 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 GC, and c) implement corrective actions as required by Canada within a timeframe agreed to with Canada.
E2.77	Incident Response	The Contractor must ensure that the security posture of the EPS 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.
E2.78	Incident Response	The SOC must a) accept e-mails from GC authorized representatives to a Contractor-provided mailbox with an auto reply to confirm receipt of the e-mail; b) acknowledge receipt of e-mails received from e-Procurement addresses authorized by Canada, within 15 minutes of receiving the e-mails 24 hours per day, 7 days per week, and 365 days per year; c) authenticate the identity of the requester using a process approved by Canada.
E2.79	Incident Response	The Contractor must create one or more Incident Tickets for each Incident it detects or reported by GC.
E2.80	Incident Response	The Contractor must physically and/or logically 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 GC dedicated storage.
E2.81	Incident Response	The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and GC-reported Incidents.
E2.82	Incident Response	The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.

E2.83	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 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.
E2.84	Incident Response	The Contractor must report all suspected or actual privacy and security violations for EPS as Security Incidents.
E2.85	Incident Response	The Contractor must provide all evidence associated to a security incident, in a COTS format specified by GC and within a mutually agreed upon time frame between Canada and the Contractor, that is associated with GC Data and relevant to the security incident including: a) results of historical Application, Network and System logs and audit records research; b) results of analysis of Application, Network and System logs and audit records; c) Application, Network and System logs and audit records; and d) additional clarification information or data as specified by GC based on the review of information provided by the Contractor under items a) to c) above
E2.86	Incident Response	The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and GC-reported Incidents.
E2.87	Incident Response	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.

E2.88	Incident Response	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 GC; 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; n) GC'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; 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).
E2.89	Incident Response	The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and GC-reported Incidents.
E2.90	Incident Response	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.
E2.91	Incident Response	The Contractor must notify the GC by email and/or telephone (e-mail and telephone number to be determined) of any incident or potential incident, once detected, that could have an impact on GC data. The GC will determine the level of injury or potential injury and determine the course of action to be taken in conjunction with the Contractor.
E2.92	Incident Response	The Contractor must not withhold from Canada any information or data in its possession that relates to EPS or is associated with a Security Incident.

E2.93	Incident Response	The Contractor must provide a secure Security Management Portal that will allow GC to view security-related information within the EPS. 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; 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).
E2.94	Incident Response	The Contractor must report all suspected or actual privacy and security violations for EPS as Security Incidents.
E2.95	Incident Response	Meetings for Security Incidents, or security related matters as identified by GC, must be in Person in the National Capital Region (NCR) or via Teleconference 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 GC.
E2.96	Incident Response	The Contractor must be available to participate in a Security Incident briefing provided by GC, (e.g. for Classified briefing).
E2.97	Incident Response	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.

E2.98	Incident Response	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 effectively maintain and mature the Security Incident response capability.
E2.99	System Maintenance	The Contractor must perform controlled maintenance by: a) scheduling, performing, documenting, and reviewing records of maintenance and repairs on EPS 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 EPS 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.
E2.100	System Maintenance	The Contractor must approve, control, monitor and maintain, on an ongoing basis, the hardware and software used for maintaining the EPS specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).
E2.101	System Maintenance	The Contractor must a) check all media containing diagnostic and test programs for malicious code before the media are used on EPS components; b) verifying that there is no EPS information contained on the equipment; c) sanitizing or destroying the EPS equipment; d) retaining the EPS equipment within the EPS facility or obtaining an exemption from a designated EPS Contracting Authority explicitly authorizing removal of the equipment from the EPS facility.

E2.102	System Maintenance	The Contractor must authorize, monitor, and control maintenance and diagnostic activities on the EPS by: a) allowing the use of maintenance and diagnostic tools approved by GC; (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 EPS by either: (i) physically and/or logically 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.
E2.103	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 EPS 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.
E2.104	Media Protection	The Contractor must provide GC with the operational security procedures that includes media protection requirements specified in this SOW.
E2.105	Media Protection	The Contractor a) must restrict access to IT media (digital and non-digital) containing EPS Data to authorized Operators; and b) employ mechanisms to audit access attempts and access granted.
E2.106	Media Protection	The Contractor must mark, in accordance with the provisions of the contract, removable IT media containing GC information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
E2.107	Media Protection	The Contractor must physically and logically control and securely store IT media containing EPS Data in accordance with: a) Industry best practices; and b) GC approved equipment, techniques, and procedures for data destruction (either on or off-site), such as but not limited to: Storage • DASCO Secure PC, Fileserver, FAX Cabinets • Mobile Shelving, Security, TAB (to G1-028) • DASCO Information Storage Cabinets

		• Secur-File (2 and 4 drawer) - ACOPS 101 • Mobile Operations Security Safe - Type A & Type B Destruction service providers • Mobile Destruction Services - Iron Mountain (MDS-35-GTI); • Destruction Facility - RECALL (Toronto facility) • Destruction Facilities - Iron Mountain (Calgary) • Mobile Destruction Services - GigaBiter LLC • Destruction Facility - Absolute Data Destruction (Toronto) Paper Shredders • Dahle 20831 EC • Kobra 400 HS ES (400 HS AO ES) • HSM 411.2 HS • Roto 600HS • Fellowes HS-1010
E2.108	Media Protection	The Contractor must employ cryptographic mechanisms to protect information in storage that are approved by GC and are in compliance with CSE guidance (ITSP.40.111 https://www.cse-cst.gc.ca/en/node/1831/html/26515).
E2.109	Media Protection	The Contractor must sanitize and verify IT media containing EPS Data, both digital and non-digital, prior to disposal, release out of The Contractor's control, or release for reuse.
E2.110	Media Protection	The Contractor must track, control and verify media sanitization by: a) performing media sanitization in compliance with ITSG-06 (https://www.cse-cst.gc.ca/en/node/270/html/10572) requirements for Protected B 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 e-Procurement Solution.
E2.111	Physical and Environmental Protection	The Contractor must provide GC with the operational security procedures that includes physical and environmental protection requirements specified in this SOW.
E2.112	Physical and Environmental Protection	The Contractor must authorize, monitor, and control all components entering and exiting the EPS facilities and maintain records of those components and activities. Records must be made available monthly and as requested by GC.

E2.113	Physical and Environmental Protection	The Contractor must implement at alternate work sites management, operational, and technical security controls that achieve the same objectives as those implemented at the main EPS Facility. Alternate site(s) must be approved concurrently with the Primary sites by CISD/IISD.
E2.114	Personnel Security	The Contractor must, upon termination of an individual's employment associated with EPS: a) terminate physical access to EPS facilities for the employee; b) terminate EPS access, including remote access; c) retrieve all security-related property (e.g., employee identity card, physical authentication token); d) upon termination of individual employment, must conduct exit interviews; and e) upon termination of individual employment must retain access to organizational information and information systems in accordance with the TBS Personnel Security Standard.
E2.115	Personnel Security	The Contractor must have access agreements to the EPS or EPS Data where: a) prior to being granted access to the EPS or EPS 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 EPS or EPS Data every two years.
E2.116	Personnel Security	The Contractor must a) prior to being granted access to the EPS or EPS 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 EPS Operators in their responsibilities to protect the privacy and confidentiality of the EPS Data as per the terms and conditions of the EPS contract and in the sanctions for failure to comply. The Contractor must provide bi-annual refresher training.
E2.117	Risk Assessment	The Contractor must provide a third party certified vulnerability test result with supporting RAW data, within a mutually agreed upon time frame between Canada and the Contractor from the date the request is made by Canada, that includes:a) physical access to the EPS facilities (i.e. Contractor's facilities where the EPS (i.e. hardware and software) is located); b) network access(es) to the EPS to allow for authenticated and unauthenticated scanning of network components and security appliances, using GC and/or industry approved and acknowledged 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 EPS (i.e., the hardware, software, and network components, security appliances, and their configuration); and (d) Limiting GC Vulnerability Assessment to discovery and scanning activities to EPS and will not engage in disruptive or destructive activities.

E2.118	System and Services Acquisition	From the date vulnerabilities are formally identified, the Contractor must expeditiously mitigate all vulnerabilities within a mutually agreed upon time frame between Canada and the Contractor.
E2.119	System and Services Acquisition	The Contractor must maintain the EPS'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 Solution and its operational environment.
E2.120	System and Services Acquisition	The Contractor must provide evidence to support authorization maintenance activities, within 30 days of a request by Canada, following all changes to the EPS within The Contractor's control.
E2.121	System and Services Acquisition	The Contractor must update, as requested by Canada, and within 30 days of a request by Canada, security operating procedures and demonstrate implementation as part of authorization maintenance.
E2.122	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 SOW and in applicable GC standards specified in this SOW.
E2.123	System and Communications Protection	The EPS must include controls to manage Denial of Service (DoS) attacks, in a manner that is consistent with leading industry practices, as agreed to by both GC and the Contractor, via the Security Assessment & Authorization (SA&A) process.
E2.124	System and Communications Protection	1) The service design for EPS must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (https://www.cse-cst.gc.ca/en/node/268/html/15236) and ITSG-38 (https://www.cse-cst.gc.ca/en/node/266/html/25034). Additionally, The EPS 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 (https://www.cse-cst.gc.ca/en/node/268/html/15236) and ITSG-38 (https://www.cse-cst.gc.ca/en/node/266/html/25034). 2) The EPS Contractor must monitor and analyze network traffic, in near real time, to detect attacks and evidence of compromised EPS components. 3) The EPS Contractor must detect attacks including but not limited to: a) ransomware attacks; b) denial of service attacks; c) malware; d) social engineering; e) unauthorized intrusion or access; f) information breach; and g) all other security breaches or cyber threats targeting GC.

E2.125	System and Communications Protection	The EPS must exclusively connect to external networks or information systems specified by Canada only through managed interfaces using boundary protection devices arranged in compliance ITSG-22 (https://www.cse-cst.gc.ca/en/node/268/html/15236) and ITSG-38 (https://www.cse-cst.gc.ca/en/node/266/html/25034).
E2.126	System and Communications Protection	The Contractor must actively manage all network connections to external services associated with the EPS 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 GC; 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.
E2.127	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 EPS from communicating outside of that communications path (e.g. accessing the Internet via a separate connection available to the device).
E2.128	System and Communications Protection	The EPS must detect extrusion events as soon as possible and Canada must be notified upon detection.
E2.129	System and Communications Protection	The Contractor must monitor and analyze hosts behaviours (Host-based Intrusion Detection and Prevention) to detect attacks and evidence of compromised hosts as soon as possible and notify Canada.
E2.130	System and Communications Protection	DELETED
E2.131	System and Communications Protection	The Contractor must configure boundary protections (i.e. firewall) to fail safe (i.e. no traffic goes through) upon failure.
E2.132	System and Communications Protection	The EPS Design a) must allow mutual authentication of connections, between the EPS and other domains as specified by Canada, and exclusively exchange information with these other domains using mutual authentication. b) Must ensure that the integrity and confidentiality of EPS Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by Canada.

E2.133	System and Communications Protection	The EPS must protect the integrity and confidentiality of EPS 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 Canada.
E2.134	System and Communications Protection	DELETED
E2.135	System and Communications Protection	The EPS Design must ensure that a) cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for EPS: 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 ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) or in a subsequent version; ii) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program) to at least FIPS 140-2 validation at Level 1, and iii) operate in FIPS Mode. b) the integrity and confidentiality of EPS Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by Canada.
E2.136	System and Communications Protection	The Contractor must not prohibit a User to encrypt, decrypt, sign and verify EPS attachment files using Certificates trusted by the GC.
E2.137	System and Communications Protection	The Contractor must only allow pre-approved mobile code in the EPS thus denying any other mobile code from being downloaded and executed.
E2.138	System and Communications Protection	The EPS component or components that collectively provide name/address resolution service for the EPS must implement internal/external role separation.
E2.139	System and Communications Protection	The EPS must allow the authentication of all types of Software Clients with a EPS credential.
E2.140	System and Communications Protection	The EPS must protect the integrity and confidentiality of EPS 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 Canada.

E2.141	System and Communications Protection	The Contractor, at their discretion, can use non-dedicated hardware, non-dedicated software for the operation, administration and management of EPS Management Data. Any use of non-dedicated hardware, non-dedicated software is only allowed for EPS Management Data according to the following conditions: a) must only allow access, process or storage of GC EPS User Data with adequate physical or logical segregation that conforms to the confidentiality, integrity and availability requirements stated in Annex 2; b) must only allow access, process or storage of GC EPS System Data with adequate physical or logical segregation that conforms to the confidentiality, integrity and availability requirements stated in Annex 2;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 EPS 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 Canada; g) must not access, process or store service design information for the EPS; and h) must not allow for the control or modification of the dedicated EPS. This does not apply to normal operational processes such as maintenance, release management, patch management, and change management.
E2.142	System and Communications Protection	The EPS must include dedicated controls for any network interconnections between dedicated and non-dedicated EPS, 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 recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. The Contractor must obtain approval from Canada for alternative physical firewall appliances;; b) incorporation of Contractor provided threat detection/prevention solutions; c) routing of traffic through authenticated proxy servers; and d) role based access control with least privilege.
E2.143	System and Communications Protection	The Contractor must physically and/or logically separate a) 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 GC dedicated storage; b) ensure that any network configuration details contained in any asset records and configuration records management systems for the EPS are encrypted.; c) the network IP traffic of the EPS System Data from all other EPS Data; and d) logically separate the network IP traffic between the EPS Management Data and the EPS User Data.
E2.144	System and Communications Protection	The categorization of data for EPS as either EPS System Data, EPS User Data or EPS Management Data will be at the sole discretion of GC and based on comparison to other similar data.
E2.145	System and Information Integrity	The Contractor must provide GC with the EPS operational security procedures that includes operational roles and responsibilities for system and information integrity requirements specified in this SOW.

E2.146	System and Information Integrity	The Contractor must define and execute the processes for patch management for the EPS 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 GC; 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 EPS 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 EPS before installation; and iii) incorporating flaw remediation into the EPS configuration management process.
E2.147	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 GC; 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 EPS.
E2.148	System and Information Integrity	The EPS must provide on priority basis, and as soon as possible, alerts (e.g. using correlation rules) following indications of compromise or potential compromise and notify Canada.
E2.149	System and Information Integrity	The EPS must prevent all non-privileged users from circumventing intrusion detection and prevention capabilities.
E2.150	System and Information Integrity	The Contractor must implement a centrally managed Integrity Verification Solution to detect unauthorized changes to software and EPS 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.
E2.151	Data Security & Information Lifecycle Management Data Inventory / Flows	The EPS 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 network and systems. In particular, Contractor must ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.

E2.152	Data Security & Information Lifecycle Management Non-Production Data	The EPS production data must not be replicated or used in non-production environments.
E2.153	Encryption & Key Management Entitlement	The EPS PKI keys must have identifiable owners (binding keys to identities) and there must be key management policies.
E2.154	Encryption & Key Management Key Generation	The EPS 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, 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 GC of changes within the cryptosystem, especially if the EPS data is used as part of the service, or the customer (tenant) has some shared responsibility over implementation of the control.
E2.155	Encryption & Key Management Sensitive Data Protection	The EPS 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.
E2.156	Encryption & Key Management Storage and Access	The EPS platform and data-appropriate encryption (in compliance with CSE guidance ITSG-111 https://www.cse-cst.gc.ca/en/node/1428/html/25015) in open/validated formats and standard algorithms must be required. Keys must not be stored in the cloud (i.e. at the EPS Cloud Contractor in question), but administered by the GC or trusted key management Contractor as mutually agreed upon with Canada. The EPS key management and key usage must be separated duties.
E2.157	Governance and Risk Management Data Focus Risk Assessments	The EPS risk assessments associated with data governance requirements must be conducted at planned intervals as mutually agreed upon with Canada and must consider the following: a) Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network; 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.
E2.158		Deleted

E2.159	Governance and Risk Management Management Program	The 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
E2.160	Governance and Risk Management Risk Management Framework	All EPS risks must be mitigated to an acceptable level. Acceptance levels based on risk criteria must be established and documented.
E2.161	Zone Internetwork Device Partitioning	The EPS use of virtual devices in the zone internetwork must be sufficiently partitioned from virtual servers in all zones for containing applications of EPS.
E2.162	Storage Partitioning	EPS Storage used by the hypervisor for virtual device images must be physically and/or logically partitioned for EPS containing applications of PROTECTED B with MEDIUM injury as defined by Canada.
E2.163	Use of Hypervisor Features	The EPS Design Specific Virtual machines must not use any machine to machine sharing mechanism (e.g. file sharing) which is implemented within the hypervisor
E2.164	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 Canada for alternative products.
E2.165	& 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 EPS.
E2.166	& Virtualization Security Production / Non-Production Environments	The EPS 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 Canada.

E2.167	& Virtualization Security Segmentation	The Contractor's multi-tenant EPS-owned or managed (physical and virtual) applications, and system and network components, must be designed, developed, deployed and configured such that provider and GC (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: a) The Contractor's 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.
E2.168	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 EPS-specific virtualization hooks available for GC review.
E2.169	Privacy Impact Assessment	As requested by the crown, the Contractor must actively participate in the conduct of a privacy impact assessment on the EPS in accordance with the TBS Privacy Impact Assessment Policy (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510).
E2.170	Physical and Environmental Protection	The Contractor must a) screen individuals prior to authorizing access to the information system in accordance with the *TBS Personnel Screening Standard*; b) Rescreen individuals according to conditions requiring rescreening; and c) For Foreign Contractors, see Part 6, 6.1(a) of Security and Privacy Requirements for Foreign Suppliers (personnel Screening).
E2.171	Physical and Environmental Protection	The Contractor must a) satisfy the personnel security control requirements including security roles and responsibilities for third-party providers. b) document personnel security control requirements. c) monitor provider compliance. d) ensure security screening of private sector organizations and individuals who have access to Protected information and assets. e) explicitly define government oversight and end-user roles and responsibilities relative to third-party provided services.
E2.172	Physical and Environmental Protection	a) The Contractor is responsible for recruitment of personnel. b) The Contractor must: • maintain an updated list which clearly identifies personnel by name, title, responsibility, completed training, and facility and systems access levels as set out in the SOW • submit the list to the Project Authority when requested. • keep an employee record file which can demonstrate that the personnel have the necessary qualifications to perform the work. Such employee record file must be submitted to the Project Authority upon request

		• Throughout the term of the contract provide the Project Authority with an updated criminal record check and credit check report for all or any personnel upon request, at the Contracting Authority's discretion. • keep the security screening documentation on file and available to the Contracting Authority for each employee for a period of ten (10) years following the initial offer of employment. • rescreens individuals according to conditions requiring rescreening.
E2.173	Operational Security	The Contractor must a) ensure that all activities carried out in relation to the Security and Privacy requirements in the Statement of Work (SOW), provides comparable levels of protection to those identified in GC policies as well as meets or exceeds industry standard or best practice (e.g. ISO 27001), whichever is greater. b) upon request by the Contracting Authority, provide proof of compliance with legislation in the country of operation which may include, but is not limited to, compliance with national laws concerning privacy protection, adherence to tax laws, incorporation regulations, labour laws. c) identify an authorized Company Security Officer (CSO) to be responsible for overseeing the privacy and security requirements of Personal Information processed as a result of the Contract. This individual will be the point of contact for privacy and security matters, in collaboration with the Contracting Authority as well as to work with the Contracting Authority for Access to Information (ATIP) requests. The CSO will be accountable for monitoring the application of privacy and security practices and responding to audit comments. Further information on the appointment of and responsibilities of a CSO can be found at: http://ssi-iss.tpsgc-pwgsc.gc.ca/msi-ism/ch1/intro-eng.html#ch1-103 . d) assign a principal IT security contact with a functional reporting relationship to security management who will ensure that the following functions are performed: i. Establish and manage the Contractor's IT security program as part of the overall security approach; ii. Identify, define and document information system security roles and responsibilities; iii. Make recommendations regarding approval of all contracts for external providers of IT security services; iv. Work with program and service delivery managers to ensure their IT security needs are met, provide advice on safeguards and advise of potential impacts of new and existing threats and on the residual risk of a program or service; v. Monitor departmental compliance with security standards; and vi. Establish an effective process to manage IT security incidents, and monitor compliance

SECTION II – SAMPLE SECURITY REQUIREMENTS TRACEABILITY MATRIX

Table 2 below provides a sample Security Requirements Traceability Matrix (SRTM).

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 EPS components; and b) provide GC 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 EPS User Accounts and Generic Accounts, as follows: a) assign a unique EPS Account and Display Name in accordance with the standard defined in SOW, 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 GC; and e) return the assigned EPS Account, Display Name, and one-time password to the Account Requester.						

ANNEX 3

PRICE SCHEDULE

Annex 3 – Price Schedule - Version 4.4

INSTRUCTIONS & NOTES

A) Bidders must quote prices in the "unshaded" area (white on monitor). The formulas located in the shaded areas (pale Yellow on monitor) are not to be changed by Bidders. Bidders must complete the tables herein and submit this annex with their proposal, and by doing so, are agreeing to the formulas and methods of calculation enclosed herein.

B) In these evaluation sheets, specific weighting factors were developed for evaluation purposes only and do not constitute any commitment by Canada.

TABLE 1

Item (A)	Description (B)	Firm Lot Price (C)	The Firm Lot Price of the EPS Transition-In must be 70% or less of the total evaluated bid price for EPS Operational
1	**EPS Transition-In**		
	Bidders must quote a Firm lot Price in Canadian dollars and in accordance with the Basis of Payment in Part 7 of the main body of the solicitation. This price must include all applicable Customs duties. Applicable Taxes are extra. Bidders should refer to section 6.10 Milestones of Annex 1 - Statement of Work for more details on each milestone. The total Firm Lot Price bid for EPS Transition-In (table 1 of Annex 3) must be 70% or less of the total evaluated bid price for EPS Operational (table 2 of Annex 3)		PASS

The payment of the EPS Transition-In Firm Lot Price will be based on the successful completion of the milestones below:

Milestones (D)	Maximum Delivery Date From Date of Contract Award (E)	Percentage of Firm Lot Price Paid Upon Completion of Milestone (F)	Milestone Payments (G = C x F)
Milestone # 1 - Operational Planning as defined in article 6.10.1 of Annex 1.	No later than the end of month 4	10%	$ -
Milestone # 2 - Solution Environment as defined in article 6.10.2 of Annex 1.	No later than the end of month 4	15%	$ -
Milestone #3 - Supplier Enablement as defined in article 6.10.3 of Annex 1.	No later than the end of month 12	15%	$ -
Milestone #4 - Contract Management as defined in article 6.10.4 of Annex 1.	No later than the end of month 18	15%	$ -
Milestone #5 - Procurement Management as defined in article 6.10.5 of Annex 1.	No later than the end of month 18	20%	$ -
Milestone #6 - Service Procurement Management as defined in article 6.10.6 of Annex 1.	No later than the end of month 24	5%	$ -
Milestone #7 - Fully Operational Baseline as defined in article 6.10.7 of Annex 1.	No later than the end of month 24	10%	$ -
Milestone #8 - Government Electronic Tendering Services (GETS) as defined in article 6.10.8 of Annex 1.	No later than the end of month 48	10%	$ -
		Total Bid Price for EPS Transition-In for Table 1	**$ -**

TABLE 2

Item (H)	Description (I)
2	**EPS Operational**

The payment of the EPS Operational (including both the Firm Lot Monthly Price and the Firm Unit Prices) is applicable after the successful completion of EPS Transition-In Milestones #1 & #2 .

For Table 2, EPS Operational, Bidders must quote either: 1) a Firm Lot Monthly Price, or 2) Firm Unit Prices, or 3) both a Firm Lot Monthly Price and Firm Unit Prices, all in Canadian dollars and in accordance with the Basis of Payment in Part 7 of the main body of the solicitation. The Firm Lot Monthly Price and Firm Unit Prices must include all applicable Customs duties. Applicable Taxes are extra. Where a Bidder quotes both a Firm Lot Monthly Price and Firm Unit Prices, the amounts for each would apply to the Basis of Payment in a resultant Contract and both would be payable for services rendered, in accordance with the Basis of Payment.

If Bidders quote Firm Unit Prices, they must do so for all three Tiers (1, 2 and 3) for one and only one of the 4 metrics (GC Users, Procurement Users, Catalogue Spend or Transactions), as defined in section 7.10.1 Basis of Payment of the RFP.

Firm Lot Monthly Price for EPS Operational:

	Number of Months for Evaluation Purposes (J)	Firm Lot Monthly Price (K)
The Firm Lot Monthly Price quoted for EPS Operational (K) is firm. However, the Firm Lot Monthly Price for EPS Operational is subject to an annual inflationary adjustment as of the first annual option period as detailed in section 7.10.1 Basis of Payment. **The amount of the EPS Operational Firm Lot Monthly Price is based on the progressive completion and acceptance by Canada of the EPS Transition-In milestones. Canada will increase the percentage of the Firm Lot Monthly Price to be paid to the Contractor. Each applicable increase will take effect in the month subsequent to the Contractor's successful completion (and Canada's acceptance) of the applicable milestone.** **The number of months used in "Number of Months During 12 Years (for evaluation purposes) (P)" equals 144 months less the highest number of months associated the applicable "Milestones (D)" in Table 1 above.**	See milestones below	

The payment of the EPS Operational Firm Lot Monthly Price will be based on the successful completion of EPS Transition-In milestones:

Milestone Completion (L)	Percentage of Firm Lot Monthly Price Paid Upon Completion of Milestone or Group of Milestones Where More Than One Appear (M)	Firm Lot Monthly Price (N=K)	Monthly Milestones Payment (O)	Number of Months During 12 Years (for evaluation purposes) (P)	Weighted Milestone Payments over 12 years (Q= O x P)
Milestone # 1 - Operational Planning AND Milestone # 2 - Solution Environment	25%	$ -	$ -	140	$ -
Milestone #3 - Supplier Enablement	15%	$ -	$ -	132	$ -
Milestone #4 - Contract Management	20%	$ -	$ -	126	$ -
Milestone #5 - Procurement Management	15%	$ -	$ -	126	$ -
Milestone #6 - Service Procurement Management	5%	$ -	$ -	120	$ -
Milestone #7 - Fully Operational Baseline	10%	$ -	$ -	120	$ -
Milestone #8 - Government Electronic Tendering Services (GETS)	10%	$ -	$ -	96	$ -
				Sub-total for Firm Lot Monthly Price for EPS Operational	**$ -**

Firm Unit Prices for EPS Operational:

The Firm Unit Prices quoted for EPS Operational (S) to (AG) are firm. However, the Firm Unit Prices for EPS Operational are subject to an annual inflationary adjustment as of the first annual option period as detailed in section 7.10.1 Basis of Payment.

Metrics	Tier 1	Tier 2	Tier 3
(R) GC Users	**< 3,500 (S)**	**3,500 to 40,000 (T)**	**> 40,000 (U)**
Monthly Firm Unit Price per GC User			
(V) Procurement Users	**< 1,250 (W)**	**1,250 to 2,500 (X)**	**> 2,500 (Y)**
Monthly Firm Unit Price per Procurement User			
(Z) Catalogue Spend (in Millions)	**< 200 (AA)**	**200 to 2,000 (AB)**	**> 2,000 (AC)**
Firm Unit Price per $1 Million in Catalogue Spend			
(AD) Transactions	**< 25,000 (AE)**	**25,000 to 250,000 (AF)**	**> 250,000 (AG)**
Firm Unit Price per Transaction			

Scenario for Evaluation Purposes Only:

The following scenario will be used for evaluation purposes only to calculate the Bidders Firm Unit Prices in Table 2. Explanations for each metric are provided, however, only the one metric bid by the Bidder will be used in the evaluation. The sum of the amounts calculated for Tier 1, 2 and 3 of the proposed metric will be the amount used for evaluation purposes.

Weighting factors will be applied to the estimated numbers and amount of all metrics to create the adjusted estimated numbers and amount per tier for evaluation purposes as follows: 38% for Tier 1, 24% for Tier 2 and 38% for Tier 3.

For the GC Users metric: The Monthly Firm Unit Price bid for each Tier will be multiplied by the adjusted estimated number of GC Users per tier for evaluation purposes, as listed below. This amount will then be multiplied by 12 to represent an annual amount. For example, for Tier 1 (S) of GC Users, a bid of $1.00 would equal to: ($1.00 X 182,400 GC Users X 12 months) = $2,188,800.00.

For the Procurement Users metric: The Monthly Firm Unit Price bid for each Tier will be multiplied by the adjusted estimated number of Procurement Users per tier for evaluation purposes, as listed below. This amount will then be multiplied by 12 to represent an annual amount. For example, for Tier 1 (W) of Procurement Users, a bid of $1.00 would equal to: ($1.00 X 11,400 Procurement Users X 12 months) = $136,800.00.

For the Catalogue Spend metric: The Firm Unit Price bid for each tier will be multiplied by the adjusted estimated amount of Catalogue Spend (in million) per tier for evaluation purposes. For example, for Tier 1 (AA) of Catalogue Spend, a bid of $1.00 would equal to: ($1.00 X 9,120 million in Catalogue Spend) = $9,120.00.

For the Transactions metric: The Firm Unit Price bid for each tier will be multiplied by adjusted estimated number of Transactions per tier for evaluation purposes. For example, for Tier 1 (AE) of Transactions, a bid of $1.00 would equal to: ($1.00 X 1,140,000 Transactions) = $1,140,000.00.

All figures provided by Canada are for evaluation purposes only and do not represent a commitment by Canada. Canada will pay the Contractor the quoted Firm Unit Price(s) for actual usage, on a monthly basis, as described in the Basis of Payment.

Tier	1	2	3
Estimated number of GC Users for the Term of the Contract for evaluation purposes		480,000	
Weighting factor for evaluation purposes	0.38	0.24	0.38
Adjusted estimated number of GC Users per tier for evaluation purposes	**182,400**	**115,200**	**182,400**
Sub-total for GC Users	$ -	$ -	$ -
Annualized sub-total for GC Users	**$ -**	**$ -**	**$ -**
Estimated number of Procurement Users for the Term of the Contract for evaluation purposes		30,000	
Weighting factor for evaluation purposes	0.38	0.24	0.38
Adjusted estimated number of Procurement Users per tier for evaluation purposes	**11,400**	**7,200**	**11,400**
Sub-total for Procurement Users	$ -	$ -	$ -
Annualized sub-total for Procurement Users	**$ -**	**$ -**	**$ -**
Estimated amount of Catalogue Spend (in Millions) for the Term of the Contract for evaluation purposes		24,000	
Weighting factor for evaluation purposes	0.38	0.24	0.38
Adjusted estimated amount of Catalogue Spend (in million) per tier for evaluation purposes	**$ 9,120.00**	**$ 5,760.00**	**$ 9,120.00**
Sub-total for Catalogue Spend	**$ -**	**$ -**	**$ -**
Estimated number of Transactions for the Term of the Contract for evaluation purposes		3,000,000	
Weighting factor for evaluation purposes	0.38	0.24	0.38
Adjusted estimated number of Transactions per tier for evaluation purposes	**$ 1,140,000.00**	**$ 720,000.00**	**$ 1,140,000.00**
Sub-total for Transactions	**$ -**	**$ -**	**$ -**
Total Evaluated Price per Tier	**$ -**	**$ -**	**$ -**
		Sub-total for Firm Unit Prices for EPS Operational	**$ -**
		Total Evaluated Bid Price for EPS Operational for Table 2	**$ -**

TABLE 3

Item (AH)	Description (AI)
3	**Professional Services**

Bidders must quote All Inclusive Daily Fixed Rates in Canadian dollars and in accordance with the Basis of Payment in Part 7 of the main body of the solicitation. All travel and living expenses must be included in the All Inclusive Daily Fixed Rates for work performed in the National Capital Region.

The All Inclusive Daily Fixed Rates quoted below are firm for the period commencing on Contract Award to March 31, 2018. For each subsequent period of one year commencing on April 1, 2018, the All Inclusive Daily Fixed Rates will be subject to annual inflation adjustment as detailed in the Basis of Payment in Part 7 of the main body of the solicitation.

A) The All Inclusive Daily Fixed Rates for each level of all categories must be priced separately and not included or bundled with other rates.

B) The All Inclusive Daily Fixed Rates for each level of all categories must be greater than $0.

C) For each category, the All Inclusive Daily Fixed Rates bid for level 1 (junior) must be at least 50% of the All Inclusive Daily Fixed Rates bid for the level 3 (senior) in the same category.

D) For each category, the All Inclusive Daily Fixed Rate for level 2 (intermediate) must be at least 60% of the All Inclusive Daily Fixed Rates bid for the level 3 (senior) in the same category.

E) Within each Grouping, the Bidder's All Inclusive Daily Fixed Rate for the lowest priced level 3 (senior) (of all professional service categories bid by the Bidder in that Grouping) must not be less than 50% of the Bidder's All Inclusive Daily Fixed Rate for the highest priced level 3 (senior) (of all professional services categories bid by the Bidder for that Grouping).

	Category (AJ)	Level (AK)	Weighting Factor for 12 Years in Days (for evaluation purposes) (AL)	All Inclusive Daily Fixed Rates (AM)	Total for 12 Years (Bid Price) (AN = AL x AM)	% of level 1 must be at least 50% of level 3	% of level 2 must be at least 60% of level 3	% of lowest level 3 must be at least 50% of highest level 3	
Group #1	Application/Software Architect	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	240		$ -		PASS		
		Level 3 - Senior	240		$ -			$0.00	
	Programmer/Software Developer	Level 1 - Junior	50		$ -	PASS			
		Level 2 - Intermediate	240		$ -		PASS		
		Level 3 - Senior	120		$ -			$0.00	
	System Analyst	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	120		$ -		PASS		
		Level 3 - Senior	240		$ -			$0.00	
	WEB Architect	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	120		$ -		PASS		
		Level 3 - Senior	240		$ -			$0.00	
	WEB Developer	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	240		$ -		PASS		
		Level 3 - Senior	20		$ -			$0.00	
	Data Conversion Specialist	Level 1 - Junior	240		$ -	PASS			
		Level 2 - Intermediate	240		$ -		PASS		
		Level 3 - Senior	120		$ -			$0.00	
	IM Architect	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	120		$ -		PASS		
		Level 3 - Senior	240		$ -			$0.00	
	Technology Architect	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	120		$ -		PASS		
		Level 3 - Senior	120		$ -			$0.00	
Group #2	Business Analyst	Level 1 - Junior	720		$ -	PASS			
		Level 2 - Intermediate	720		$ -		PASS		
		Level 3 - Senior	1400		$ -			$0.00	
	Business Process Re-engineering (BPR) Consultant	Level 1 - Junior	720		$ -	PASS			
		Level 2 - Intermediate	720		$ -		PASS		
		Level 3 - Senior	1400		$ -			$0.00	
	Business Transformation Architect	Level 1 - Junior	1400		$ -	PASS			
		Level 2 - Intermediate	1400		$ -		PASS		
		Level 3 - Senior	2800		$ -			$0.00	
	Change Management Consultant	Level 1 - Junior	1400		$ -	PASS			
		Level 2 - Intermediate	1400		$ -		PASS		
		Level 3 - Senior	2800		$ -			$0.00	
	Organizational Development Consultant	Level 1 - Junior	480		$ -	PASS			
		Level 2 - Intermediate	480		$ -		PASS		
		Level 3 - Senior	480		$ -			$0.00	
Group #3	IT Security Analyst	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	120		$ -		PASS		
		Level 3 - Senior	120		$ -			$0.00	
	IT Security Engineer	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	20		$ -		PASS		
		Level 3 - Senior	20		$ -			$0.00	
	IT Security Design Specialist	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	20		$ -		PASS		
		Level 3 - Senior	20		$ -			$0.00	
	Network Security Analyst	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	20		$ -		PASS		
		Level 3 - Senior	20		$ -			$0.00	
	IT Security VA Specialist	Level 1 - Junior	20		$ -	PASS			
		Level 2 - Intermediate	80		$ -		PASS		
		Level 3 - Senior	20		$ -			$0.00	

Total Evaluated Bid Price for Professional Services for Table 3	**$ -**

GROUP #1	
Lowest level 3	$0.00
Highest level 3	$0.00
	PASS

GROUP #2	
Lowest level 3	$0.00
Highest level 3	$0.00
	PASS

GROUP #3	
Lowest level 3	$0.00
Highest level 3	$0.00
	PASS

TABLE 4

Item (AO)	Description (AP)	Weighting Factor in Number of Tender Feeds (for evaluation purposes) (AQ)	Firm Lot Price (AR)	Total (Bid Price) AS = AQ x AR
4	**Optional Work - Tender Feeds**			
	Bidders must quote a Firm lot Price per Tender Feed in Canadian dollars and in accordance with the Basis of Payment in Part 7 of the main body of the solicitation. This Firm Lot Price must include all applicable Custom duties. Applicable Taxes are extra. **The Firm Lot Price quoted for Optional Work - Tender Feeds (AM) is firm. However, the Firm Lot Price for Optional Work-Tender Feeds is subject to an annual inflationary adjustment as of the first annual option period as detailed in section 7.10.1 Basis of Payment.**			
	Firm Lot Price per feed integration	13		$ -
	Total Evaluated Bid Price for Optional Work for Table 4			**$ -**

TABLE 5.1

Optional Work - Financial Management

INSTRUCTIONS

A) During the Term of the Contract, Canada has the option to request the services described in section 7.2.6 - Functional Requirements: SECTION F - FINANCIAL MANAGEMENT of Annex 1 for any, a combination of or all Instances listed below.

B) Financial Management Transition-In

Bidders must quote a Firm Lot Price per DFMS Instance for Financial Management Transition-In in Canadian dollars in accordance with the Basis of Payment in Part 7 of the main body of the solicitation. The prices must include all applicable Customs duties. Applicable taxes are extra. The Firm Lot Price per DFMS Instance will only be paid upon successful completion and Canada's acceptance of the Work described in section 7.2.6. Functional Requirements: SECTION F - FINANCIAL MANAGEMENT of Annex 1 to the portfolio of the applicable instance listed below. There is no milestone payment associated with the Firm Lot Prices below.

C) The Firm Lot Prices quoted for Optional Work - Financial Management (AR) are firm. However, the Firm Lot Prices for Optional Work - Financial Management are subject to an annual inflationary adjustment as of the first annual option period as detailed in section 7.10.1 Basis of Payment.

Item (AT)	DFMS Instance (AU)	Participating Clients per specific DFMS Instance (AV)	Firm Lot Price per DFMS Instance for Financial Management Transition-In (AW)
5.1	Agriculture and Agri-Food Canada (AAFC)	Agriculture and Agri-Food Canada Canadian Pari-Mutual Agency Canadian Food Inspection Agency Canadian Dairy Commission Natural Resources Canada Environment Canada	
5.2	Canadian Border Services Agency (CBSA)	Canadian Border Services Agency	
5.3	Canadian Heritage (CH)	Canadian Heritage Parks Canada	
5.4	Canada Revenue Agency (CRA)	Canada Revenue Agency Canada Revenue Agency - Revenue Ledger	
5.5	Canadian Space Agency (CSA)	Canadian Space Agency	
5.6	Immigration, Refugees and Citizenship Canada (IRCC)	Immigration, Refugees and Citizenship Canada Passport Canada	
5.7	Global Affairs Canada (GAC)	Global Affairs Canada Canadian International Trade Tribunal Export Development Corporation	
5.8	Employment and Social Development Canada (ESDC)	Employment and Social Development Canada	
5.9	Health Canada (HC)	Health Canada Hazardous Material Information Review Commission Patented Medicine Prices Review Board Assisted Human Reproductive Agency of Canada Public Health Agency of Canada Indigenous and Northern Affairs Canada	
5.10	Innovation, Science and Economic Development Canada (ISEDC)	Innovation, Science and Economic Development Canada Canadian Intellectual Property Office Office of Infrastructure Canada Copyright Board	
5.11	Department of Justice (DoJ)	Department of Justice Public Prosecution Service of Canada	
5.12	National Research Council (NRC)	National Research Council	
5.13	Department of National Defence (DND)	Department of National Defence	
5.14	Public Works and Government Services Canada (PWGSC)	Public Works and Government Services Canada Shared Services Canada	
5.15	Royal Canadian Mounted Police (RCMP)	Royal Canadian Mounted Police Public Safety & Emergency Preparedness Canada	
5.16	Treasury Board Secretariat (TBS)	Treasury Board Secretariat Finance Canada Public Appointments Commission Secretariat Privy Council Office Security Intelligence Review Committee Canada School of Public Service Canadian Transport Agency Office Superintendent Financial Institutions Canada	
5.17	Fisheries and Oceans Canada	Fisheries and Oceans Canada	
5.18	Correctional Services Canada	Correctional Services Canada	
5.19	Transport Canada	Transport Canada	
5.20	GC Financial Management (GCFM) Instance (SAP S4/Hana)	Atlantic Canada Opportunities Agency Canadian Human Rights Commission Canadian Intergovernmental Conference Secretariat Canadian Transportation Accident Investigation and Safety Board (o/a Transportation Safety Board of Canada) International Joint Commission Office of the Auditor General of Canada Office of the Commissioner of Lobbying Office of the Information Commission Office of the Privacy Commission Office of the Public Sector Integrity Commissioner Western Economic Diversification Canadian Institutes of Health Research Canadian Nuclear Safety Commission Canadian Radio-television and Telecommunications Commission Courts Administration Service Economic Development Agency of Canada for the Regions of Quebec Financial Transactions and Reports Analysis Centre of Canada Library and Archives Canada Library of Parliament Public Service Commission National Energy Board Natural Science and Engineering Research Council Office of the Commissioner for Federal Judicial Affairs Office of the Chief Electoral Officer Office of the Conflict of Interest and Ethics Commissioner Office of the Co-ordinator - Status of Women Parole Board of Canada Office of the Governor General's Secretary PPP Canada (Public Infrastructure, Public Transit, Public Private Partnership) Registrar of the Supreme Court of Canada Senate Ethics Officer The Senate Veterans Affairs Canada Canadian Centre for Occupational Health and Safety Canadian High Arctic Research Station Military Grievances External Review Committee Military Police Complaints Commission of Canada Office of the Communications Security Establishment Commissioner Office of the Commissioner of Official Languages The National Battlefield Commission Statistics Canada	

Total for DFMS Instance Financial Management Transition-In	**$** -

TABLE 5.2	
Volume Discount for DFMS Instance	
Instructions	
DFMS Instance Financial Management Transition-In **1) Where Canada requests that more than one DFMS instance receive the functionalities described in 7.2.6 - Functional Requirements: SECTION F - FINANCIAL MANAGEMENT of Annex 1 in the same request, the Functional Management Transition-In Firm Lot Price for the applicable DFMS instances will be discounted at the applicable percentage quoted below.**	
Number of DFMS instances included in the request for Financial Management functionalities (AX)	**Discount (reduction) applicable to each DFMS instance Financial Management Transition-In Firm Lot Price in the request (AY)**
1	
2	
3	
4	
5 to 9	
10 to 15	
16 or more	
Average discount for evaluation purposes	0%

Total for DFMS Instance Financial Management Transition-In from table 5.1	$ -
Average discount to DFMS Instance Financial Management Transition-In Firm Lot Price from table 5.2	0%
Evaluated discounted price for DFMS Instance Financial Management Transition-In	**$** -

TABLE 6.1

Optional Work - DFMS Instances for EPS

INSTRUCTIONS

A) During the Term of the Contract, Canada has the option to on board any, a combination of or all Instances listed below into EPS as defined in article 7.2.7 of Annex 1.

B) DFMS Instance EPS Transition-In

Bidders must quote a Firm Lot Price per DFMS instance in Canadian dollars in accordance with the Basis of Payment in Part 7 of the main body of the solicitation. The prices must include all applicable Customs duties. Applicable taxes are extra. The Firm Lot Price per DFMS instance will only be paid upon successful deployment of the EPS to the portfolio of the applicable instance listed below. There is no milestone payment associated with the Firm Lot Prices below.

C) The Firm Lot Prices quoted for Optional Work - DFMS Instances for EPS (AW) are firm. However, the Firm Lot Prices for Optional Work - DFMS Instances for EPS are subject to an annual inflationary adjustment as of the first annual option period as detailed in section 7.10.1 Basis of Payment.

Item (AZ)	DFMS Instance (BA)	Participating Clients per specific DFMS Instance (BB)	Firm Lot Price per DFMS instance for EPS Transition-In (BC)
6.1	Agriculture and Agri-Food Canada (AAFC)	Agriculture and Agri-Food Canada Canadian Pari-Mutual Agency Canadian Food Inspection Agency Canadian Dairy Commission Natural Resources Canada Environment Canada	
6.2	Canadian Border Services Agency (CBSA)	Canadian Border Services Agency	
6.3	Canadian Heritage (CH)	Canadian Heritage Parks Canada	
6.4	Canada Revenue Agency (CRA)	Canada Revenue Agency Canada Revenue Agency - Revenue Ledger	
6.5	Canadian Space Agency (CSA)	Canadian Space Agency	
6.6	Immigration, Refugees and Citizenship Canada (IRCC)	Immigration, Refugees and Citizenship Canada Passport Canada	
6.7	Global Affairs Canada (GAC)	Global Affairs Canada Canadian International Trade Tribunal Export Development Corporation	
6.8	Employment and Social Development Canada (ESDC)	Employment and Social Development Canada	
6.9	Health Canada (HC)	Health Canada Hazardous Material Information Review Commission Patented Medicine Prices Review Board Assisted Human Reproductive Agency of Canada Public Health Agency of Canada Indigenous and Northern Affairs Canada	
6.10	Innovation, Science and Economic Development Canada (ISEDC)	Innovation, Science and Economic Development Canada Canadian Intellectual Property Office Office of Infrastructure Canada Copyright Board	
6.11	Department of Justice (DoJ)	Department of Justice Public Prosecution Service of Canada	
6.12	National Research Council (NRC)	National Research Council	
6.13	Department of National Defence (DND)	Department of National Defence	
6.14	Public Works and Government Services Canada (PWGSC)	Public Works and Government Services Canada Shared Services Canada	
6.15	Royal Canadian Mounted Police (RCMP)	Royal Canadian Mounted Police Public Safety & Emergency Preparedness Canada	
6.16	Treasury Board Secretariat (TBS)	Treasury Board Secretariat Finance Canada Public Appointments Commission Secretariat Privy Council Office Security Intelligence Review Committee Canada School of Public Service Canadian Transport Agency Office Superintendent Financial Institutions Canada	
6.17	Fisheries and Oceans Canada	Fisheries and Oceans Canada	
6.18	Correctional Services Canada	Correctional Services Canada	
6.19	Transport Canada	Transport Canada	
6.20	GC Financial Management (GCFM) Instance (SAP S4/Hana)	Atlantic Canada Opportunities Agency Canadian Human Rights Commission Canadian Intergovernmental Conference Secretariat Canadian Transportation Accident Investigation and Safety Board (o/a Transportation Safety Board of Canada) International Joint Commission Office of the Auditor General of Canada Office of the Commissioner of Lobbying Office of the Information Commission Office of the Privacy Commission Office of the Public Sector Integrity Commissioner Western Economic Diversification Canadian Institutes of Health Research Canadian Nuclear Safety Commission Canadian Radio-television and Telecommunications Commission Courts Administration Service Economic Development Agency of Canada for the Regions of Quebec Financial Transactions and Reports Analysis Centre of Canada Library and Archives Canada Library of Parliament Public Service Commission National Energy Board Natural Science and Engineering Research Council Office of the Commissioner for Federal Judicial Affairs Office of the Chief Electoral Officer Office of the Conflict of Interest and Ethics Commissioner Office of the Co-ordinator - Status of Women Parole Board of Canada Office of the Governor General's Secretary PPP Canada (Public Infrastructure, Public Transit, Public Private Partnership) Registrar of the Supreme Court of Canada Senate Ethics Officer The Senate Veterans Affairs Canada Canadian Centre for Occupational Health and Safety Canadian High Arctic Research Station Military Grievances External Review Committee Military Police Complaints Commission of Canada Office of the Communications Security Establishment Commissioner Office of the Commissioner of Official Languages The National Battlefield Commission Statistics Canada	

Total for DFMS Instance EPS Transition-In	**$ -**

TABLE 6.2

Volume Discount for DFMS Instance

Instructions

DFMS Instance EPS Transition-In

1) Where Canada requests more than one DFMS instance to be deployed in the same request, the EPS Transition-In Firm Lot Price for the applicable DFMS instances will be discounted at the applicable percentage quoted below.

Number of DFMS instances included in the request (BD)	Discount (reduction) applicable to each DFMS instance EPS Transition-In Firm Lot Price in the request (BE)
1	
2	
3	
4	
5 to 9	
10 to 15	
16 or more	

Average discount for evaluation purposes	0%

Total for DFMS Instance EPS Transition-In from table 6.1	$	-
Average discount to DFMS Instance Transition-In Firm Lot Price from table 6.2		0%
Evaluated discounted price for DFMS Instance EPS Transition-In	**$**	**-**

TABLE 7
Summary

Description (BF)	Total Bid Price (BG)	Overall Weighting Factors (BH)	BEV (BI = BG x BH)
Table 1 - EPS Transition-In	$ -	1.00	$ -
Table 2 - EPS Operational	$ -	1.00	$ -
Table 3 - Professional Services	$ -	0.80	$ -
Table 4 - Optional Work - Tenders Feed	$ -	1.00	$ -
Table 5 - Evaluated discounted price for DFMS Instance Financial Management Transition-In	$ -	1.00	$ -
Table 6 - Evaluated discounted price for DFMS Instance EPS Transition-In	$ -	1.00	$ -
Total Evaluated Bid Price	**$ -**		
		Total Bid Evaluated Value (BEV)	**$ -**

ANNEX 4

SECURITY REQUIREMENTS CHECK LIST (SRCL) & SECURITY CLASSIFICATION GUIDE (SCG)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN578131350 REV #6
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	☑	☐
Not releasable / À ne pas diffuser	☐	
Restricted to: / Limité à :	☐	☐
Specify country(ies): / Préciser le(s) pays :	Please refer to Annex 1 - List of approved Countries by ISP	
All NATO countries / Tous les pays de l'OTAN	☐	
Restricted to: / Limité à :	☐	
Specify country(ies): / Préciser le(s) pays :		
No release restrictions / Aucune restriction relative à la diffusion		☐
Restricted to: / Limité à :		☐
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 : _____

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 matérial 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 Intenet), 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 récapitulaif.

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	Protected Protégé B	Protected Protégé 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).

Terms and Definitions

Table 1 below summarizes the terms as used within this SCG and associated definitions. The definition herein do not replace the definitions listed in General Conditions 2035 or other definitions listed throughout the Contract articles.

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**.
Generic Accounts	Are any accounts within the proposed **EPS** solution that are non-unique. A typical user account is unique and assigned to a specific user while the generic accounts are used by multiple users or system processes.
Host	Means any Internet Protocol (IP) addressable entity connected to an IP-based network.

Table 1: Definitions

Term	Definition
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.
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.

Table 1: Definitions

Term	Definition
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 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	• Business Data;	Both (refer to information flow	N/A[1]	N/A	No	EPS Contractor	These are external users of the EPS	These EPS end users will be processing, accessing and handling information specific to

[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
	delegates who will need to access the information specific to their business and bid responses including company proprietary information.	• User credentials (each supplier has ownership of the assigned unique users accounts); • RFP submissions and associated supplier propriety information; • Supplier's financial information	IF-A, IF-D, IF-E in Figure 3 below)					representing the supplier community.	their company including pricing and proposal information in response to the GC tenders.
3.	Any EPS Contractor personnel with physical access to the EPS infrastructure at Contract Service Delivery Points (SDP), includes	• Physical hardware; • Service Delivery Point (Data Center Contractor / SSC);	Canada (refer to information flow IF-C in Figure 3 below)	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	This is for any Contractor personnel including facilities management resources that have physical access to the EPS hardware	SSC/Contractor SOC is dedicated for SSC internal services and associated resources. SSC/Contractor most likely will not allow 3rd party resources to be collocated in SSC/Contractor SOC facilities. The EPS deployment model will involve use of SSC/Contractor

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
	Contractor data centers, Security Operations Center (SOC), Network Operations Center (NOC). Additionally, physical segregation requirements will be separately identified within the EPS Contract.	• Data as stored on the Contractor's local Backup Media						equipment at the Contractor SDP for SOC/NOC capabilities that will be separate from SSC SOC/NOC.	Data Center facilities. The access to these facilities and infrastructure elements will be considered privileged access requiring the designated level of clearance. 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 permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up and recovery,

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
									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 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; • COTS products configuration details;	Both (Information Flow not applicable here)	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	Typically Subject Matter Expert's from outside of Canadian Operations are likely 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
		• Hardware details; • Security policy and rules as applicable to EPS including perimeter controls and auditing						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	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-attacks on the EPS and supporting infrastructure.

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
		applicable to EPS including perimeter controls and auditing							
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	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
								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.	
7.	Contractor Security Operations Center(SOC) Personnel	• All Business Data; • Security Data including audit logs; • System configuration including security	Canada (refer to information flow IF-C in Figure 3 below)	Protected 'B'	Enhanced Reliability	Yes	EPS Contractor	All SOC personnel will have privileged access to EPS infrastructure and sensitive security incident data. Contractor SOC personnel will need	SSC/Contractor SOC is dedicated for SSC/Contractor internal services and associated resources. SSC most likely will not allow 3rd party resources to be collocated in SSC/Contractor SOC facilities. Given the privileged access to IT/IS resources from within SOC infrastructure, any unauthorized access through this trusted back door function

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; • Physical hardware; • Service Delivery Point (Data Center Contractor / SSC); • Backup Media						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.	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 with permissions such as may be required for the purpose of maintenance, monitoring, detection, back-up and recovery, testing, installation and configuration changes

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
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'	Enhanced Reliability	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,	SSC/Contractor SOC is dedicated for SSC internal services and associated resources. SSC/Contractor most likely will not allow 3rd party resources to be collocated in SSC/Contractor SOC facilities. 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

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
								these resources will have intimate knowledge of the security configurations for various components, including security components, within the EPS.	• 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 ; • System configurat ion	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 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.

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
		including security components; • Reporting; • Service Delivery Point (Data Center Contractor); • Incident ticketing system							
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	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	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 functions (typically referred to as local maintenance).

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
		Point (Data Center Contractor); • Incident ticketing system						operational life of the EPS, the 4th Level OEM resources will not have direct access to EPS or 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.	

ANNEX 5

GLOSSARY

1.0 GLOSSARY OF TERMS

This section outlines key terms that are employed throughout *Annex 1 – Statement of Work (SOW)* and *Annex 2 – Security and Privacy*. This annex should be used in conjunction with Annex 6 – Acronyms. The definition herein do not replace the definitions listed in General Conditions 2035 or other definitions listed throughout the Contract articles.

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: Is a document that describes the tests scenarios, activities, and expected results.

Access Control: Security Controls that support the ability to permit or deny access to resources within the EPS.

Access Right(s): An approach to control, regulate or restrict system access to a User according to the User's assigned role(s) and rights.

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 specifically to answer a single, business question.

Ad hoc Approver: Is a role assigned, on a case by case basis, to define an additional level of approval throughout the approval process.

Automated Attendant: Includes a series of recorded messages describing actions that a caller can take to access particular services. An auto-attendant can route multiple simultaneous phone calls to the appropriate person.

Authorized Administrator: Is a role defined for managing advanced system functionalities in the EPS. Such as configuration of business rules, workflows, etc.

Authorized User: A role that is given authorization to perform privileged operations in the EPS. Such as issuing RFx, contracts, contract management, etc. This may include users that are designated to maintain the solution and could potentially include the Contractor's support team.

Analytics: 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.

Application Availability: The percentage of time the 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.

Authentication: Process to verify the digital identity of the sender of a network communication.

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 management method to compare the performance of like products or services.

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 has been elected by the GC to be closed for business.

Business Intelligence (BI): The set of techniques and tools for the transformation of raw data into meaningful and useful information for business analysis purposes.

Business Number: A unique identifying number that is given to a registered business by the Canada Revenue Agency.

Back to TOP

C

Call Abandonment Rate: Parameter to measure the percentage of all inbound Service Desk calls in the queue (e.g. 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.

Canadian Broader Public Sector: any province or municipality in Canada, any Canadian aid agency or public health organization, or any Canadian academic or health institution.

Catalogue: Combines all defined Framework Agreements, Business Rules, ordering rules, and attributes from within Catalogue Data File(s) during the ordering process.

Catalogue Attribute: is a feature or property of a good or service (e.g. Size, Price, Colour, Part #, etc.) which is searchable to a user accessing the associated Catalogue. These attributes will be configured by authorized users when creating the Catalogue Data File.

Catalogue Data File: The electronic file where Suppliers and Authorized Users provide the required information on goods and services which can be purchased by Users in the e-Catalogue. Each Catalogue Data File is linked to a specific Framework Agreement.

Ceiling Price: The maximum price to be paid to the contractor as established in the contract and beyond which the contractor will not receive additional compensation for the defined work.

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 Order: An amendment to an existing Order.

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.

Classification Level: An indicator of the sensitivity of the EPS information (e.g. Protected A, Protected B, Unclassified, and other classifications specified by Government of Canada (GC)).

Client: A public sector Department, Agency, Crown Corporation, and Broader Public Sector.

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.

Comprehensive Land Claims Agreements (CLCAs): 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.

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 modified, out-of-the-box without having to customize, to meet the GC services standards and requirements including IT architecture, functional, performance, availability, maintainability, security, Business Continuity, and Disaster Recovery.

Consumer-Like: Providing a business to consumer experience.

Contract Award Notice (CAN): Notification 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).

Contract Lifecycle Management (CLM): The process of systematically and efficiently managing Contract creation, execution, management of the contract, and analysis to maximize operational and financial performance and minimize risk.

Contract Repository: A repository that facilitates the flow (e.g. 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.

Contractor Facility: A Data Center, Security Operations Center (SOC), Help Desk and any supporting service hosted within a Contractor's facility.

Control Test Environment: is the equivalent of a User Acceptance Test (UAT) or Pre-Prod environment.

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.

Credentials Management: 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.

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, Near 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: 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: A system used for reporting and data analysis. Data Warehouses 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 communicate information clearly and efficiently to Users (e.g., a map is a way to visualize which areas of the country get the most rainfall).

Delegate: Any person who is granted authorization to act on behalf of another User 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.(e.g.: bandwidth attack, distributed denial of service, backscatter, consumption of system resource attack, communication obstruction, disruption of state information, disruption to routing or DNS information and web defacement).

Departmental Financial and Materiel Management System (DFMS): The financial management system(s) used by a Client; 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.

Directed Procurement Process: Is the process of awarding a contract to Suppliers without competition in accordance with the Government Contracts Regulations.

Disposition: A range of processes associated with implementing retention, destruction or transfer decisions which are documented in disposition or other instruments.

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.

Back to TOP

E

e-Catalogue: This is the graphical version of the Catalogue presented to the User when they seek to buy goods or services. It contains the list of searchable fields and attributes to assist Users in finding what they need and to add it to their Shopping Cart.

e-Sourcing: A function that uses secure, web-enabled, collaborative tools to conduct strategic activities in the procurement lifecycle online, including identifying suitable Suppliers, requirements definition, tendering, negotiation, Contract award and Contract management.

Electronic Data Interchange (EDI): Refers to the process of transferring data from one system directly into another.

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 for Suppliers to submit a bid electronically.

Email Response Time: Parameter to measure the time for the EPS Contractor 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 Contractor's response is logged in the EPS.

Enterprise Service Bus (ESB): A software architecture model used for designing and implementing communication between software applications in a service-oriented architecture (SOA).

EPS Data: All data associated with EPS, including User Data, Operational Data.

EPS Infrastructure: All hardware, systems software, and facilities that process and manage the EPS.

EPS Management Data: Any data derived from the operation, administration and management of the EPS that the Contractor directly uses for:

a) service requests;
b) incident tickets (excluding security incident tickets);
c) billing records and invoices at an organizational level (not user level);
d) asset records;
e) configuration records;
f) system performance, capacity and resource planning information; and
g) alarms and events (excluding security alarms and events).

EPS System Data: Any data that the Contractor uses to control or modify the operation, administration and management of the EPS which includes:

a) security incidents;
b) security information and events management (SIEM);
c) network perimeter management (e.g. firewall);
d) intrusion and prevention management;
e) AV/AS and malware protection;
f) hypervisor and virtual machine systems management;
g) network management and operations;
h) system configuration files, logs and scripts;

i) authentication, authorization and accounting systems;
j) disk systems;
k) management service;
l) service delivery portal;
m) capacity and resource management systems;
n) software distribution, updates and patches; and
o) directory services.

EPS User Data: Includes Account, Notifications, Customized views and filters.

Back to TOP

F

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 (e.g. 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 and live chat 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 must 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), which 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.

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

Generic accounts: any accounts within the EPS that are non-unique. A typical user account is unique and assigned to a specific user while the generic accounts are used by multiple users or system processes.

Ghost Card: Is a credit card number that is tied to a specific contract or Framework Agreement that is set by an Authorized User in order to allow numerous Users to use this Ghost Card for their orders.

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.

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

Host: Means any Internet Protocol (IP) addressable entity connected to an IP-based network.

Back to TOP

I

Identity Credential and Access management (ICAM): An EPS service, owned and managed by the Contractor 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 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.

Incoterm: A set of rules which define the responsibilities of sellers and buyers for the delivery of goods under sales contracts for domestic and international trade. An internationally recognized standard used worldwide, published by the International Chamber of Commerce (ICC).

Information Protection Centre (IPC): Is the GC's point of contact for security incidents.

Integration: The process of bringing together the component subsystems into one system and ensuring that the subsystems function together as a system.

International Bilateral Industrial Security Instruments: The Industrial Security Program (ISP) negotiates International Bilateral Industrial Security Instruments such as arrangements, Memoranda of Understanding, etc. with other nations. These instruments concern the exchange and safeguarding of Protected and Classified information and assets. Canada's international allies recognize the ISP's International Industrial Security Directorate (IISD) as the Designated Security Authority (DSA) for industrial security.

Interoperability: The ability for different systems and applications to communicate, exchange data, and use the information that has been exchanged.

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.

Invitational Competitive: Is the process of inviting Suppliers to participate in a Solicitation process to bid when it is not an Open Competitive process. Generally only those Suppliers that are invited can participate.

Invitation To Tender (ITT): A bid Solicitation type that is used 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.

Item Master Record: Stores unique information about a Catalogue item within a Catalogue File.

Back to TOP

J-K

Jurisdictions: 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. The Knowledge Base provides the insight, rationale and/or justification for making an informed decision.

Knowledge Management: Knowledge Management is the process which institutionalizes best practices, training materials, and organizational policies for quick and easy access.

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.

Malware: 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.

Master Record: Original record from which subsequent copies are made.

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 that is used to pay for services performed or goods delivered. The Method of Payment types include: Progress Payments; Advance Payments; Holdbacks; Single Payment; Monthly Payment; Milestone Payment.

Method of Supply: See Framework Agreement.

Method of Supply Limitation – Individual Supplier: The maximum dollar amount that a Supplier can receive in Contracts or Orders against a specific Method of Supply.

Method of Supply Limitation – Cumulative Limitation: The maximum dollar amount that all Suppliers can receive in Contracts or Orders against a specific Method of Supply.

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 or deliverable.

Mobile Code: A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.

Back to TOP

N

Near Real-Time: Data that is active and is at the given point in time being worked on in the EPS.

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".

Notice: An electronic advertisement that solicits goods or services, indicates that a Solicitation is being updated or changed, or announces a Contract award.

Notification: A system generated message informing a User of an action required (e.g. approve, deny) or that an action has been completed that requires attention.

Back to TOP

O

One-Time Login: A feature and capability of EPS that minimizes the requirement for additional User account logins to the various EPS services and components. The feature assigns a role-based access to all components of the EPS after a successful login by the User using credentials such as a user id and password.

Open Competitive: Is a publically advertised solicitation.

Open Data: Is a practice that makes data easily available to the public in order to enable re-use of the data.

Operations Center: Contractor location that includes infrastructure and resources required for the centralized management and operation of the EPS.

Operator: Is a resource performing System Administrator duties on behalf of the Contractor.

Order: A purchase issued against a Method of Supply in accordance with the applicable terms and conditions.

Order Threshold: The maximum dollar amount that a User can issue an Order without seeking the approval of the User responsible for the Method of Supply.

Other Government Departments (OGD): Any Department and Agency other than Public Works and Government Services Canada

Back to TOP

P

Patch Management: Standardized methods and procedures to minimize the impact of problems for the EPS.

Payment Method: is the way in which Users pay for the items that they purchase. (e.g. direct deposit, ghost card, virtual card)

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 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 contractor's resource.

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.

Portal: 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 Authorized User to establish a price threshold where the Supplier can increase or decrease their price, without seeking approval from the contracting officer (e.g. -30% + 30%). If the price they are proposing is not in this threshold it will trigger a notification to advise the Authorized User.

Problem Management: Standardized methods and procedures to minimize the impact of problems.

Process Management: 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.

Procurement Business Number (PBN): Is a unique identifier that is assigned to each Supplier that is based on the Business Number assigned by Canada Revenue Agency.

Procurement File: a case file consisting of a grouping of procurement information and documents related to a specific procurement.**Procurement Process:** This process addresses the acquisition of goods and services from requisition to payment.

Production System: 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 Users of such Systems.

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: The special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

PunchOut: Is a system functionality that connects a buyer to a Supplier's external web site from within the EPS.

Purchase Order: Is a contract type that includes all the terms and conditions, which is typically used for low dollar value procurements that are not a result of a Solicitation or a Catalogue.

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: 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.

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.

Release Management: Standardized methods and procedures for the integration and flow of development, testing, deployment, and support of the EPS.

Remote Access: Access to the EPS through an external network (e.g. the Internet).

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.

Repository: An electronic location for safely storing or preserving information for re-use within the EPS.

Request for x (RFx): is a generic term to describe the different types of sourcing events, which include: 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 Standing Offer (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 Supply Arrangement (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 currently 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 goods or services and authority to commit funds to for the initiation of the contract or Framework Agreement.

Reverse e-Auction: Is an online function between auctioneers and bidders, which takes place on an electronic marketplace. 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 requirements stipulated in the Solicitation document.

Root Cause Analysis: Describes a wide range of approaches, tools, and techniques used to uncover causes of problems.

Back to TOP

S

Scalability: The ability of a system, network, or process to handle a varying workload in a capable manner or its ability to be enlarged to accommodate 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: A strategy performance management tool - a semi-standard structured report, supported by design methods and automation tools that can be used to keep track of the execution of activities and to monitor the consequences arising from these actions

Sealed Bid: A document enclosed in a sealed envelope and is submitted in response to a RFx. 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: The ability to permit or deny User access to resources within the EPS.

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 or 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.

Service Desk Availability: The required time frames during which services provided by the Service Desk must be available to Users.

Service Desk Reporting: The activities associated with the preparation of and access to Service Desk reports that are based on defined criteria.

Service Oriented Architecture (SOA): 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.

Shopping Cart: An electronic "basket" used for holding items until the User submits the Shopping Cart for approval, which then becomes a Shopping Cart Request. The Shopping Cart serves as an intermediary step between a User searching a catalogue and placing an Order.

Shopping Cart Request: Contains all the information required for a Shopping Cart to be processed for approval.

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: A unique internal number that is assigned to a Solicitation that is generated by 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.

Sourcing Event: A sourcing process that includes understanding the need; evaluating the supply market; developing an appropriate strategy; executing that strategy, usually involving market interactions such as the issue of an RFP and/or negotiation; selecting supplier(s); and developing a contractual agreement.

Spend: The percentage of total enterprise spend (which includes all direct, indirect, and services spend) that a procurement organization manages or influences.

Spend Data: Expenditure data captured (e.g. date of payment, reference number, type of payment, item, cost) during the lifecycle of a procurement process which can be used to determine a complete picture of procurements made within the Government of Canada.

Spend Analysis: A software- and service-based technique for collecting, cleansing, classifying and analyzing spend data.

Standing Offer (SO): An offer from a 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.

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.

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 Users of the EPS that will be using the solution to offer their services in response to various tenders published by GC.

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 Repository: A library of electronic documents and specific information linked to a Supplier 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 used throughout the EPS.

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 (e.g. 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): A non-binding agreement between PWGSC and a Supplier who is pre-qualified to provide goods or services to the Government of Canada.

System Administrator: Is a role defined for the technical upkeep, configuration, and secure operation of the EPS.

Back to TOP

T

Task Authorization: Administrative document that allows a User to authorize a contractor to conduct work on an "as and when requested" basis in accordance with the terms and conditions of a Contract with Task Authorization.

Taxonomies: A way to classify and assign a structure to information.

Technology Architecture: 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. Sometimes referred to as contingent labour service.

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 Users.

Trainer: An individual who is responsible for teaching details relating to a service(s).

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 (e.g. 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: Any person that is registered with an account to use the EPS.

User Categories
System Administrator: (Operator) Is a role defined for the technical upkeep, configuration, and secure operation of the EPS.
Authorized Administrator: Is a role defined for managing advanced system functionalities in the EPS. Such as configuration of business rules, workflows, etc.
Authorized User: A role that is given authorization to perform privileged operations in the EPS. Such as issuing RFx, contracts, contract management, etc.
User: (GC User, Supplier) Any person that is registered with an account to use the EPS.

User Profile: Is a record of User-specific data that defines the User's working environment and roles.

Back to TOP

V

Virtual Card: Is a credit card number that is tied to a GC User. Purchases made on each of these cards are then charged back to the department to which the card was issued.

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 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 information along a prescribed process path associated with a particular service or good. The processes are 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 Users, 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 Annex 5 – Glossary. This document also complements the contractual terms and conditions that will appear in the solicitation and resulting contract.

Acronym	Description
AA	Automated Attendant
ABAC	Attribute-Based Access Control
AIT	Agreement on Internal Trade
AB	Acquisitions Branch
AP	Acquisition Program
API	Application Programming Interface
BF	Bring Forward
BI	Business Intelligence
BPEL	Business Process Execution Language
BPM	Business Process Management
BPS	Broader Public Service
CAD	Computer-Aided Design
CEDI	Common Enterprise Data Initiative
CIOB	Chief Information Officer Branch
CISD	Canadian Industrial Security Directorate
CLCA	Comprehensive Land Claims Agreements
CLM	Contract Lifecycle Management
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and Related Technology
COTS	Commercial Off-the-Shelf
CPI	Consumer Price Index
CPU	Central Processing Unit
CRA	Canada Revenue Agency
CRL	Certificate Revocation List
CSI	Construction Specific Institute
CSV	Comma Separated Values
CWBS	Contract Work Breakdown Structure
DFMS	Departmental Financial & Materiel Management Systems
DND	Department of National Defence
DR	Disaster Recovery
DSP	Drawing and Specification Packages
DW	Data Warehouse
EDI	Electronic Data Interchange
EPS	e-Procurement Solution
ERP	Enterprise Resource Planning

Acronym	Description
ESB	Enterprise Service Bus
ETL	Extract, Transform and Load
EU	European Union
FMS	Financial and Material Systems
FMT	Financial Management Transformation
FPOC	First Point of Contact
FY	Fiscal Year
GC	Government of Canada
GCDOCS	Government of Canada Electronic Document Record Management Solution
GCIF	Government of Canada Interoperability Framework
GETS	Government Electronic Tendering Service
GL	General Ledger
GSIN	Goods and Services Identification Number
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IAM	Identity and Access Management
IBISI	International Bilateral Industrial Security Instruments
ICAM	Identity, Credential and Access Management
ICAS	Internal Centralized AuthenticationService
ID	Identification
IP	Intellectual Property
IPC	Information Protection Centre
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
ITT	Invitation to Tender
JMS	Java Message System
JV	Joint Venture
JSON	JavaScript Object Notation
KM	Kilometres
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOI	Letter of Intent
MSRP	Message Session Relay Protocol (or Manufacturer's Suggested Retail Price)
NAFTA	North American Free Trade Agreement
NATO	North Atlantic Treaty Organization

Acronym	Description
NCR	National Capital Region
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OGD	Other Government Departments
OLAP	On-line Analytical Processing
P2P	Procure-to-Pay
PCI DSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
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
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"
RSS	Really Simple Syndication
SAs	Supply Arrangements
SaaS	Software as a Service
SAML 2.0	Security Assertion Markup Language
SAP	Systems, Applications and Products
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
SOW	Statement of Work
SRCL	Security Requirements Check List
SRM	Supplier Relationship Management
SSC	Shared Services Canada
TAs	Task Authorizations
TB	Treasury Board

Acronym	Description
TBD	To be Determined
TBS	Treasury Board Secretariat
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 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 bids received in response to this bid solicitation. 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 responsive bid receives the highest combined Technical Score and Financial Score will be recommended for award of a Contract.

3. Evaluation Weighting

Evaluation Element	Proposal Element	Weight
Technical Score	Technical Bid – Point-Rated Criteria	7,000 points
Financial Score	Financial Bid	3,000 points
	TOTAL	10,000 points

4. Evaluation Process

The e-Procurement Solution (EPS) bid evaluation team will conduct the evaluation of the bids including the Supply Chain Security Information (SCSI) Assessment, the Technical Bid Evaluation and the Financial Bid Evaluation as described in section *4.2 Bid Evaluation* of the RFP. The evaluation is comprised of the following:

a) The SCSI will be assessed in accordance with section 5. *Supply Chain Security Information (SCSI) Assessment* of this attachment.

b) The Bidders' technical bid will be evaluated and technical points will be assessed in accordance with section 6. *Technical Evaluation* of this attachment.

c) The Bidders' financial bid will be evaluated and financial points will be assessed in accordance with section 7. *Financial Evaluation* of this attachment.

d) Canada will combine the Bidder's Technical Score and Financial Score to determine the Bidder with the highest combined Technical Score and Financial Score.

e) Canada will conduct a Proof of Proposal (PoP) test on the Bidder who obtained the highest combined Technical Score and Financial Score to test compliance of the proposed solution with the requirements of this bid solicitation. The Bidder must successfully pass the PoP test. If the Bidder fails the PoP Test, it will be deemed non-responsive and given no further consideration. Canada will then proceed with the PoP Test for the Bidder with the next highest combined Technical Score and Financial Score.

Canada reserves the right to conduct any element of the evaluation process concurrently or out of sequence. Where a Bidder is declared non-responsive for any portion of the evaluation process, Canada may end the evaluation process for that bid.

Bids will be evaluated individually in accordance with this bid solicitation and its Annexes, Attachments, and Forms.

Bidder's information required to evaluate bids must not be provided through references (i.e. web sites or other documents). Any such information must be provided with the Bidder's bid. Canada will not consider information that is solely provided though references (i.e. web sites or other documents).

5. Supply Chain Security Information (SCSI) Assessment

5.1. Definitions

The following words and expressions used in this SCSI Assessment 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, 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 requested to be done, delivered or performed by the Contractor under the resulting contract.

5.2. Mandatory Supply Chain Security Information (SCSI) Submission Requirements

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

5.2.2. Bidders must submit, with their bid, the following SCSI:

Notice to Bidders: *Due to the Software-as-a-Service (SaaS) nature of this solution, the Bidder is required to provide only the Network Diagrams and List of Subcontractors details, rather than each IT product used by each subcontractor. However, if specific supporting IT products are to be used by the Bidder itself, those details must be provided in the IT Product List tab in Form 3 to Part 4 – SCSI - IT Product List and Subcontractor List Form.*

5.2.3. 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:

a. 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.);

b. 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;

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

d. Product Model Name or Number: identify the advertised name or number of the Product by the Product Manufacturer and/or Software Publisher;

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

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

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

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).

5.2.4. Network Diagrams: Bidders must provide one or more conceptual network diagrams that collectively show the complete network proposed to be used to deliver the services described in Annex 1 – 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. Refer to Attachment 4 to Part 4 – Supply Chain Scope Diagram. As a minimum the diagram must show the following key nodes for the delivery of the services under the resulting contract of this solicitation process to the role of the Bidder and, if applicable, subcontractor(s):

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.

5.2.5. List of Subcontractors: Bidders 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.

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.

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.

6. Technical Evaluation

The Technical Evaluation includes the mandatory technical criteria and the point-rated criteria.

6.1 Mandatory Technical Requirements

For both *Step 1 – Preliminary Technical Evaluation* and *Step 2 – Final Technical Evaluation* (refer to sections 4.2.2.1 and 4.2.2.2 of the RFP), the bids will be assessed for their compliance with the mandatory technical criteria identified in *Attachment 2 to Part 4 – Technical Evaluation.*

Bidders must meet all of the mandatory technical criteria in order to be considered responsive. Failure to meet all mandatory technical criteria will result in the bid being deemed non-responsive and it will be excluded from further consideration.

6.2 Point-Rated Criteria

For both *Step 1 – Preliminary Technical Evaluation* and *Step 2 – Final Technical Evaluation* (refer to sections 4.2.2.1 and 4.2.2.2 of the RFP), each bid will be rated by assessing a technical score, rounded to two decimal points, to each point-rated criteria as identified in Attachment 2 to Part 4 – Technical Evaluation. The degree of importance of each point-rated criteria is determined by the points allocated to each criterion.

Bidders must meet all pass marks as identified in Attachment 2 to Part 4 – Technical Evaluation, including the overall minimum pass mark, in order to be considered technically responsive. Failure to meet all pass marks in *Step 2 – Final Technical Evaluation* will result in the bid being deemed non-responsive and it will be excluded from further consideration.

6.2.2 Reference Checks

6.2.2.1. Canada reserves the right to contact reference(s) for verification or validation of what the Bidder has proposed in its bid.

6.2.2.2. The Bidder should provide a third-party reference as requested in Attachment 2 to Part 4 – Technical Evaluation, using Form 2 to Part 4 – Project Reference Check Form. If the information requested in Form 2 to Part 4 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 may be submitted.

6.2.2.3. 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.

6.2.2.4. 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. However, if the client contact is unable to provide the reference check in writing, the client contact may provide the reference check verbally. 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.

6.2.2.5. 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 identify his or her willingness and availability to conduct such reference check. If Canada has not received the required acknowledgement from the client contact within 2 working days, 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 10 working days. The client contact's failure to respond to Canada's request within 10 working days (or a longer period otherwise specified in writing by the Contracting Authority) will result in non-consideration of the Bidder's claimed project experience.

6.2.2.6. Notwithstanding subsection 6.2.2.4, if the client contact responds that he or she 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 responds that he or she is unavailable. The process described in 6.2.2.4 is also 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 6.2.2.3.

6.2.2.7. 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.

6.2.2.8. A Bidder will not pass the reference check if:

a. the client contact fails to respond to Canada's request within 10 working days (or a longer period otherwise specified in writing by the Contracting Authority);
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 remains contradictory to the project reference information, even after clarification with the Bidder; or
d. the client contact organization and/or client contact is currently a team member (parent organization, affiliated organization, any subsidiary organization and subcontractors) of the Bidder.

6.2.2.9. A Bidder who has failed in any reference check, as a result of 6.2.2.7, for the mandatory technical criteria at Attachment 2 to Part 4, will be deemed not fully meeting the mandatory requirements and will be declared non-responsive.

6.2.2.10. A Bidder who has failed in any reference check, as a result of 6.2.2.7, for the point-rated criteria at Attachment 2 to Part 4, will not be awarded the points associated with the respective rated criterion that is subject to the reference check. If the Bidder does not

meet all the minimum pass mark(s) for the point-rated criteria, its bid will be declared non-responsive.

6.3 Technical Score

The Technical Score will be calculated by adding the points for the Technical Evaluation – point-rated criteria.

7. Financial Evaluation

The points for the Financial Evaluation will be allocated as per this section.

7.1 Mandatory Financial Criteria

For both *Step 1 – Preliminary Evaluation of the Mandatory Financial Criteria (MFC 1)* and *Step 2 – Final Evaluation of the Mandatory Financial Criteria (MFC 1)* (refer to section 4.2.3.1.1 and 4.2.3.1.2 of the RFP), the bids will be assessed for their compliance with the mandatory financial criterion MFC 1 identified below.

For both *Step 1 – Preliminary Evaluation of the Mandatory Financial Criteria (MFC 2 – MFC 10)* and *Step 2 – Final Evaluation of the Mandatory Financial Criteria (MFC 2 – MFC 10)* (refer to section 4.2.3.2.1 and 4.2.3.2.2 of the RFP), the bids will be assessed for their compliance with the mandatory financial criteria MFC 2 to MFC 8 identified below.

Bidders must meet all of the mandatory financial criteria in order to be considered responsive. Failure to meet all mandatory financial criteria in either *Step 2 – Final Evaluation of the Mandatory Financial Criteria (MFC 1) or Step 2 – Final Evaluation of the Mandatory Financial Criteria (MFC 2 – MFC 10)*, will result in the bid being deemed non-responsive and it will be excluded from further consideration.

MFC 1	Bidders must bid a complete financial proposal.
MFC 2	Bidders must bid all prices and rates in Canadian dollars and bid in accordance with the Price Schedule described in Annex 3.
MFC 3	The total Firm Lot Price bid for EPS Transition-in (table 1 of Annex 3) must be less than 70% of the total bid price for EPS Operational (table 2 of Annex 3)
MFC 4	The All Inclusive Daily Fixed Rates for each level of all categories (table 3 in Annex 3) must be priced separately and not included or bundled with other rates.
MFC 5	The All Inclusive Daily Fixed Rates for each level of all categories (table 3 of Annex 3) must be greater than $0.
MFC 6	For each category, the All Inclusive Daily Fixed Rates bid for level 1 (junior) must be at least 50% of the All Inclusive Daily Fixed Rates bid for the level 3 (senior) in the same category (table 3 of Annex 3).
MFC 7	For each category, the All Inclusive Daily Fixed Rate for level 2 (intermediate) must be at least 60% of the All Inclusive Daily Fixed Rates bid for the level 3 (senior) in the same category (table 3 of Annex 3).
MFC 8	For each grouping, the Bidder's All Inclusive Daily Fixed Rate for the lowest priced level 3 (senior) (of all professional service categories bid by the Bidder) must not be less than 50%

	of the Bidder's All Inclusive Daily Fixed Rate for the highest priced level 3 (senior) (of all professional services categories bid by the Bidder).
MFC 9	The Bidder must provide a cost breakdown of its EPS Transition-In Firm Lot Price and its EPS Operational Firm Lot Monthly Price. The breakdown should be detailed and include a breakdown of the costs into constituent elements such to permit insight into the costs and costing structure within each of these prices.
MFC 10	For EPS Operational (table 2 of Annex 3), if Bidders quote Firm Unit Prices, they must do so for all three Tiers (1, 2 and 3) for one and only one of the 4 metrics (GC Users, Procurement Users, Catalogue Spend or Transactions), as defined in section 7.10.1 Basis of Payment of the RFP.

7.1.1 Financial Bids

All Bidders that have met all mandatory requirements (not including the PoP Test) of this solicitation, including being deemed technically responsive, will have their financial bid evaluated to determine its financial score. The Pricing Schedule in Annex 3 will be used to determine the Total Bid Evaluated Value (BEV). The BEV of each bid will be evaluated in Canadian dollars, Applicable Taxes excluded, FOB destination, Canadian customs duties and excise taxes included.

7.1.2 Formulae in Pricing Tables

Where the pricing tables provided to Bidders in Annex 3 – Price Schedule include any formulae, Canada may re-input the prices provided by Bidders into a fresh table with the formulae as per the issued RFP, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a Bidder.

7.1.3 Financial Score Evaluation

a. The BEV for each responsive Bidder will be added together and divided by the number of responsive Bidders to calculate the average (Mean Amount).

b. Then, a Normalized Raw Score will be determined by application of the following formula:

Normalized Raw Score = 1 – Absolute value of ((Mean Amount – BEV) ÷ Mean Amount)
OR
= 1 – | (Mean Amount – BEV) ÷ Mean Amount|

The Normalized Raw Score measures the Bidder's BEV against the average of all Bidders' BEV.

c. A Correction Factor will then be used, rounded to three decimal points, to favour lower total bid prices. The Bidder with the lowest BEV will receive 100% of its Normalized Raw Score. All other Bidders will have their Correction Factor prorated against the Bidder with the lowest BEV, rounded to no decimal points. The following formula will be applied:

% for Correction Factor for all other Bidders = (Lowest BEV / Bidder's BEV) X 100

d. Lastly, points will be assigned, rounded to two decimal points, based on the following formula:

Financial Score = Normalized Raw Score X Correction Factor X 3000

Example

Example of 4 bids received in response to this RFP (numbers are only for illustrative purposes and in no way representative of expected pricing by Canada):

Bidder A:

Item	Applicable Fee	Subtotal
1	BEV for EPS Transition-In	$5,000,000
2	BEV for EPS Operational	$6,000,000
3	BEV for Professional Services	$1,000,000
4	BEV for Optional Work – Tender Feed	$1,000,000
5	Evaluated discounted price for DFMS Instance Financial Management Transition-In	$500,000
6	Evaluated discounted price for DFMS Instance EPS Transition-In	$1,500,000
Total Bid Evaluated Value (adding subtotals for items 1 through 6)		$15,000,000

Bidder B:

Item	Applicable Fee	Subtotal
1	BEV for EPS Transition-In	$5,000,000
2	BEV for EPS Operational	$7,000,000
3	BEV for Professional Services	$1,500,000
4	BEV for Optional Work – Tender Feed	$500,000
5	Evaluated discounted price for DFMS Instance Financial Management Transition-In	$1,000,000
6	Evaluated discounted price for DFMS Instance EPS Transition-In	$2,000,000
Total Bid Evaluated Value (adding subtotals for items 1 through 6)		$17,000,000

Bidder C:

Item	Applicable Fee	Subtotal
1	BEV for EPS Transition-In	$2,500,000
2	BEV for EPS Operational	$4,500,000
3	BEV for Professional Services	$1,000,000
4	BEV for Optional Work – Tender Feed	$1,000,000
5	Evaluated discounted price for DFMS Instance Financial Management Transition-In	$250,000
6	Evaluated discounted price for DFMS Instance EPS Transition-In	$750,000
Total Bid Evaluated Value (adding subtotals for items 1 through 6)		$10,000,000

Bidder D:

Item	Applicable Fee	Subtotal
1	BEV for EPS Transition-In	$7,000,000
2	BEV for EPS Operational	$13,000,000
3	BEV for Professional Services	$3,000,000
4	BEV for Optional Work – Tender Feed	$1,000,000
5	Evaluated discounted price for DFMS Instance Financial Management Transition-In	$2,000,000
6	Evaluated discounted price for DFMS Instance EPS Transition-In	$4,000,000
Total Bid Evaluated Value (adding subtotals for items 1 through 6)		$30,000,000

Results:

	BEV	Deviation	Normalized Raw Score	Correction (%)	Score (out of 3000)
Bidder A	$15,000,000	$(3,000,000)	0.833	67%	1674.33
Bidder B	$17,000,000	$(1,000,000)	0.944	59%	1670.88
Bidder C	$10,000,000	$(8,000,000)	0.556	100%	1668.00
Bidder D	$30,000,000	$12,000,000	0.333	33%	329.67
Total of all Bids				$72,000,000	
Average (Mean)				$18,000,000	
Number of Bidders				4	

7.1.4 Scoring for Only Two Proposals

In the event that only two bids are deemed technically responsive (including the mandatory technical and point-rated criteria), the calculations for the scores will be as follows:

The bids with the lowest BEV will be awarded 3000 financial points. The remaining bid will have its BEV prorated against the lowest BEV, rounded to two decimal points. The following formula will be applied:

Financial Score = (Lowest BEV / Bidder's BEV) X 3000

Example
Example of 2 bids received in response to this RFP (numbers are only for illustrative purposes):

Bidder	Total Evaluated Proposal Price	Financial Score
Bidder A	$18,000,000.00	($16,000,000.00/$18,000,000.00) * 3000 = 2670.00
Bidder B	$16,000,000.00	($16,000,000.00/$16,000,000.00) * 3000 = 3000.00

8. Proof of Proposal (PoP) Test

i. Through the Proof of Proposal (PoP) Test, the Bidder must demonstrate how its proposed solution meets certain technical and functional requirements described in Annex 1 – Statement of Work.

ii. After being notified by the Contracting Authority that a PoP Test will take place, the Bidder will be given a maximum of 5 working days to prepare for the PoP Test. During this five day preparation window, the Bidder may visit Canada's PoP test site during one of these five days, between 9:00 a.m. and 5:00 p.m., as part of its preparations. The Bidder should refer to Attachment 3 to Part 4 – PoP Test for details on the requirements to be demonstrated during the PoP Test. The proposed solution must be complete and functional at that point in time to the extent required to demonstrate the requirements described in the PoP Test.

iii. The Bidder must perform the PoP Test on-site in the offices of Public Works and Government Services Canada (PWGSC) in the Ottawa/Gatineau area.

iv. Canada will make available two large monitors along with HDMI video cables set up in the testing site, to which the Bidder may connect its laptop(s) to allow the evaluators to clearly see the screen and the demonstrated test results. The Bidder must bring its own laptop(s) to be used during the PoP Test and is responsible for their technical performance. It may use more than one laptop during the test. Canada will not provide a laptop. The Bidder is also responsible for providing any additional equipment and material necessary and the necessary testing data to complete its PoP Test and at its own cost.

v. The Bidder must provide its own internet connectivity for the PoP Test. Canada will not be providing internet connectivity. Should Canada be responsible for any delays in the testing process, as determined by Canada, the Bidder will be provided makeup time equivalent to the time lost to complete the PoP Test.

vi. Immediately following the 5 day preparation window, the Bidder will be given a maximum of 2 working days to complete and demonstrate compliance with the requirements of the PoP Test. If the Bidder wishes to use some of this time to further prepare for the PoP Test, this will be permitted. A Bidder may repeat the PoP Test as many times as it wishes during these 2 days allocated for testing. A day is defined as 9:00 a.m. to 5:00 p.m. and access to the room shall be limited to these times, subject to delays as described in v. The time limits described herein will be strictly followed.

vii. The Bidder must keep confidential any information it receives from Canada regarding the PoP Test.

viii. If Canada determines that the proposed solution does not meet the requirements of the PoP Test, the Bidder will fail the PoP Test and the bid will be declared nonresponsive.

9. Basis of Selection

9.1. To be declared responsive, a bid must:

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

b. Pass the SCSI Assessment;

c. Meet all the mandatory technical criteria under Attachment 2 to Part 4;

d. Obtain all minimum pass marks for the point-rated criteria under Attachment 2 to Part 4;

e. Meet all the mandatory financial criteria; and

f. Successfully pass the Proof of Proposal Test.

Bids not meeting 9.1. *a.* to *f.* will be declared non-responsive, and receive no further consideration.

9.2 The Bidder with the responsive bid with the highest combined Technical Score and Financial Score will be recommended for award of a Contract. In the event two or more responsive bids have the same highest combined Technical Score and Financial Score, the responsive bid that obtained the highest Technical Score will be recommended for award of a Contract.

9.3 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.

9.4 The table below illustrates an example where all four bids are responsive and the selection of the Contractor is determined by combining the Technical Score and Financial Score.

Basis of Selection - Highest Combined Rating (10,000 points) of Technical Score (70%) and Financial Score (30%)

Bidder	Bidder A	Bidder B	Bidder C	Bidder D
Technical Score (TS)	6500/7000	6750/7000	5500/7000	6900/7000
Financial Score (FS)	1674.33/3000	1670.88/3000	1668.00/3000	329.67/3000
Combined Rating (CR = TS + FS)	8174.33	8420.88	7168.00	7229.67

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 Technical 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**			**700**	**420**
R1.1	Solution Management Services – Additional				
	Section A	*	440		
	Section B	1	190		
R1.2	SAP Certified Partner Solution	*	70		
R2	**Implementation Plan**			**1400**	**840**
R2.1	Implementation Plan	2	730		
R2.2	Training Plan	2	390		
R2.3	Change Management and Communication Plan	2	280		
R3	**Management Approach**			**1750**	**1050**
R3.1	Organizational Structure and Use	2	280		
R3.2	Risk Management	2	280		
R3.3	Relationship Management	2	280		
R3.4	Service Desk Support	2	350		
R3.5	Innovation and Value Added	2	350		
R3.6	Product Roadmap	2	210		
R4	**Technical Approach**			**1050**	**630**
R4.1	Technical Deployment Model - SaaS	2	350		
R4.2	Technical Architecture	2	350		
R4.3	Technical Integration	2	175		
R4.4	IT Service Continuity Plan	2	175		
R5	**Security Plan**			**1050**	**735**
R5.1	Policies and Procedures (Controls)	2	157.5		

R5.2	IT Security Topology Diagram	2	87.5		
R5.3	Security Organization	2	105		
R5.4	Data Segregation	2	140		
R5.5	Disposal	2	105		
R5.6	Continuous Monitoring Program Services	2	140		
R5.7	Industry IT Security Certifications	2	157.5		
R5.8	Identity, Credential and Access Management	2	157.5		
R6	Additional Functional Requirements			1050	525
R6.1	General	*	51		
R6.2	Portal Requirements	*	27		
R6.3	Sourcing and Contract Management	*	232		
R6.4	Procurement Management	*	279		
R6.5	Service Procurement	*	133		
R6.6	Business Intelligence	*	72		
R6.7	Supplier Relationship Management	*	160		
R6.8	Data Information Management	*	93		
R6.9	User Management	*	3		
Overall Maximum Points & Pass Threshold:				**7000**	**4200**

Notes:

[1]Refer to the Technical Evaluation Scales included at section 4 of this attachment.

*These criteria do not use a scale. These criteria have points assigned to specific elements. Refer to the applicable criteria for additional detail on scoring.

2. Evaluation of Experience of Bidder's Team Members

a. For the purposes of the mandatory technical criteria under section *3. Mandatory Technical Criteria* (M1 & M2) and point-rated criteria *R1 Corporate Experience* (R1.1 & R1.2) under section *4. Point-Rated Criteria*, the definition of "Bidder" under section *04 Definition of Bidder* of Standard Instructions 2003 is replaced with the following definition of Bidder:

> *"Bidder" means the 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 also includes the parent, subsidiaries or other affiliates of the Bidder, its subcontractors and association of entities*.*

**An "Association of Entities" means separate legal entities within a formally organized professional services network, where all members of the network operate using a common brand, with shared access to intellectual property and talent resources and integrated technology, methodology, strategies and policies across the network.*

b. For the purpose of this solicitation, a "team member" is the entity whose experience is being used to meet evaluation criteria M1, M2 R1.1 and R1.2. Where a Bidder cites the experience of a team member, Canada will only consider this experience if the experience is accessible to the Bidder and the Bidder can rely upon and use the experience in the performance of any resulting Contract. The Bidder is required to demonstrate this accessibility through the certification provided under Table 7 of Form 1 to Part 4 – RFP Submission Form. Experience listed without providing any supporting data to describe where, how and by whom such experience was obtained or failure to demonstrate that the Bidder has a teaming agreement with the team member whose experience satisfies the requirement may result in the experience not being considered for evaluation purposes. The experience identified by the Bidder to meet specific criterion must be for Work for which the Bidder, as defined in 2.a. above, was directly responsible.

3. Mandatory Technical Criteria

Each bid will be reviewed for compliance with the following mandatory technical criteria. Bids that do not comply with each and every mandatory technical criteria will be declared non-responsive and not considered further.

No.	Evaluation Area	Bid Submission Requirements	Evaluation Criteria	Applicable Scale
M1	EPS Management Services	The Bidder should 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 in Part 3 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 in Part 3 of the SOW;	The Bidder must clearly demonstrate experience in the provision of an e-procurement solution of similar nature and scope to at least the following sections as described in Part 3 of the SOW: o 3.2.1 Section A: General Requirements - Workflow; o 3.4 Section C: Sourcing and Contract Management; o 3.5 Section D: Procurement Management; o 3.9 Section H: Supplier Relationship Management; and o 3.11 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. Project Reference using Form 2 to Part 4 – Project Reference Check Form.	(c) the e-procurement solution must have had a minimum of 5,000 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 April 11th, 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 in Part 3 of the SOW; and (e) a minimum of 7,500 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 in Part 3 of the SOW. The Bidder must have been the prime contractor responsible for the provision of the services of the e-procurement solution. For the purpose of this criterion, internal User mean an individual who is employed by the client or a representative of the client and had access to the solution. For the purpose of this criterion, the term "Contract" includes contracts with Task Authorizations, Standing Offers, Supply Arrangements, and non-Catalogue Purchase Orders. Amendments will not count towards the number of contracts. The definition of "Contract" does not include Orders issued under a Catalogue, including	

			Call-ups under a Standing Offer and Task Authorizations under a contract with Task Authorizations.	
M2	Data Residency and Personnel	The Bidder should clearly demonstrate its EPS data residency compliance and provide a data center deployment plan(s) which should include specifics on: i. location(s) (country and city) of primary data center(s); ii. location(s) (country and city) of secondary data center(s) and backup centers; iii. location(s) (country and city) of all the infrastructure components (including, but not limited to, database servers, SANS, application servers); and iv. location(s) (country and city) of the SOC, NOC and the Service Desk. The Bidder should clearly demonstrate its EPS business entities and personnel location compliance and provide: i. location(s) (country and city) of all business entities performing Work under the Contract; and ii. location(s) of all personnel performing the Work under the Contract.	The Bidder must demonstrate that the EPS datacenters, EPS software, EPS middleware, the EPS Service Desk, SOC and NOC infrastructure and Data for the entire EPS reside within Canada and/or countries with which Canada has international bilateral industrial security instruments (IBISI). The Bidder must demonstrate that the personnel for the entire EPS, including SOC, NOC and Service Desk be physically located and operate within Canada, countries with which Canada has IBISI, or within countries belonging to EU or NATO. The Bidder must demonstrate that all business entities be physically located, be legally authorized to operate and to do business and be registered, where the local legislation requires such registration, within Canada, countries with which Canada has IBISI, European Union and/or NATO countries.	

4. Point-Rated Criteria

Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the table and scales below and the scoring grid in section 1 – "Evaluation Summary". Each point-rated criterion should be addressed separately.

Table 1 – Point Allocation for Section A of criterion R1.1			
Percentage of Aggregate Target	**Number of Internal Users (aggregate target of 100,000)**	**Dollar Value in Orders (aggregate target of $5,000,000,000.00)**	**Number of Contracts (aggregate target of 50,000)**
< 50% of aggregate target	0 points	0 points	0 points
50% to < 60% of aggregate target	44 points	88 points	88 points
60% to < 70% of aggregate target	52.8 points	105.6 points	105.6 points
70% to < 80% of aggregate target	61.6 points	123.2 points	123.2 points
80% to < 90% of aggregate target	70.4 points	140.8 points	140.8 points
90% to < 100% of aggregate target	79.2 points	158.4 points	158.4 points
100% of aggregate target	88 points	176 points	176 points

Scale 1 – Demonstrated Experience	
0	**Not Addressed** – No response provided or the response does not address this solicitation requirement.
1	**Minimally Addressed** – The bid fails to demonstrate the experience requested due to significant deficiencies. The deficiencies or weaknesses demonstrate that the Bidder did not meet the similarity and relevancy on the scope. The Bidder demonstrates limited experience and the experience is of little relevance to the solicitation requirements.
2	**Partially Addressed** – The bid does not demonstrate that the Bidder met all of the similarity and relevancy on the scope due to a significant level of deficiencies or weaknesses. However, the Bidder has some similarity and relevancy on the scope and demonstrates experience of some relevance to the solicitation requirements.
3	**Satisfactorily Addressed** – The bid does not demonstrate that the Bidder met all of the similarity and relevancy on the scope due to a moderate level of deficiencies or weaknesses. However, the Bidder has an acceptable level of the similarity and relevancy on the scope and demonstrates experience of adequate relevance to the solicitation requirements.
4	**Very Well Addressed** – The bid demonstrates that the Bidder met most of the similarity and relevancy on the scope with few deficiencies or weaknesses. The Bidder has a very good level of the similarity and relevancy on the scope and demonstrates experience that is very relevant to the solicitation requirements.
5	**Excellently Addressed** – The bid demonstrates that the Bidder met all of the similarity and relevancy on the scope with very few or no deficiencies or weaknesses. The Bidder has an excellent level of the similarity and relevancy on the scope 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 bid 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. Bid poses a perceived large residual risk* to Canada.
2	**Partially Addressed** – The bid 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. Bid poses a perceived medium residual risk* to Canada.
3	**Satisfactorily Addressed** – The bid 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. Bid poses a perceived medium-low residual risk* to Canada.
4	**Very Well Addressed** – The bid 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. Bid poses a perceived low residual risk* to Canada.
5	**Excellently Addressed** – The bid 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. Bid 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.

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 bid obtains a 3 in the evaluation of R-2.1, then the Bidder's score for that criterion would be calculated as follows:

Score of 3 = 60%
Weight of criteria R.2.1 – Implementation Plan = 730 points
Therefore, 60% x 730 points = 438 points

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 scope 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	**Section A:** 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 achieving the aggregate targets in successfully delivering services of similar nature and scope as this solicitation and: (a) had 100,000 internal Users with access to the production system of the e-procurement solution; (b) had $5,000,000,000 (CAD, taxes extra, foreign currency will be based on the Bank of Canada daily noon exchange rate on April 11th, 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

		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 *section 3.4 – Sourcing and Contract Management* of the SOW; 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. The description of 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 projects submitted for R1.1 must not include the project the Bidder submits for criterion M1. If it is included in response to this rated criterion, it will not be considered. If more than 5 projects are proposed, only the first 5 projects in the order of presentation will be evaluated.	the services described in the Procurement Management section of the SOW; and (c) had 50,000 Contracts that must have been awarded in the e-procurement solution through services similar in nature and scope to the services described in *section 3.4 – Sourcing and Contract Management* of the SOW. *For Section A, the points awarded will be the sum of the points obtained for each aggregate target in accordance with Table 1.* **Section B:** For the projects evaluated in Section A, in addition to evaluating the aggregate targets of the Bidder's projects as evaluated above, Canada will evaluate the similarity and relevancy of the scope of each 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 April 11th, 2016); (d) the solution was implemented for a public sector client; (e) the solution was delivered as a Software as a Service; (f) the solution implemented integrated with the client's SAP finance system; (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 been contractually responsible for the provision of the services of the e-procurement solution. For the purpose of this criterion, internal Users mean an individual who is employed by the client or a representative of the client and had access to the solution. For the purpose of this criterion, the term "Contract" includes contracts with Task Authorizations, Standing Offers, Supply Arrangements, and non-Catalogue Purchase Orders. Amendments will not count towards the number of contracts. The definition of "Contract" does not include Orders issued under a Catalogue, including Call-ups under a Standing Offer and Task Authorizations under a contract with Task Authorizations. *For Section B, the projects will be evaluated in accordance with Scale 1. The final score for Section B will be determined by giving a single score for all of the projects combined.*
R1.2	SAP Certified Partner Solution	The Bidder should provide one of the following: i. for the Bidder, an SAP certified partner certification; ii. for the Bidder's EPS software, an SAP certified partner solution certification; iii. confirmation that the Bidder's proposed EPS is an SAP product i. .	Canada will evaluate based on the following: (a) the Bidder is an SAP certified partner = 70 points (b) the EPS proposed by the Bidder is an SAP certified partner solution = 70 points (c) confirmation that the Bidder's proposed EPS is an SAP product = 70 points (d) the Bidder is not an SAP certified partner, the EPS proposed by the Bidder is not an SAP certified partner solution or the Bidder did not provide confirmation that the Bidder's proposed EPS is an SAP product = 0 points

			Maximum of 70 points.
R2	**Implementation Plan**		
R2.1	Implementation Plan	The Bidder should submit its Implementation Plan that describes its proposed approach to the EPS implementation to meet the requirements of this solicitation, including implementation of the complete EPS, all optional services listed in the RFP, 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, 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 major task;	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.

		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 its 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 Milestones as outlined in 6.10 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 objectives and requirements in sections 6.7.3 and 6.7.4 of Annex 1 - Statement of Work of this solicitation, including: i. a description of the approach used for initial training and regenerative training for each of the User communities;	Canada will evaluate the degree to which the Bidder's training approach is feasible and consistent with the 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 will be effective for training all types of Users 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

		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.	(d) the use of industry best 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 types of User; 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 and communication demonstrate that: (a) it increases awareness to the various types of Users during the implementation and roll-out of the EPS; (b) it encourages adoption by the various types of User during roll-out; and (c) it is feasible and takes into consideration GC Legislation and Policies as described in Part 2 of the SOW.
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 an efficient, effective and responsive organizational model and by considering: (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 efficiency to Canada;

		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 which are relevant to the position; 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 team members; 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 and team members 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;	(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.

		vii. indicating how the proposed organization will address the requirements of this solicitation; and 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 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 and/or its impact. 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:	Canada will evaluate the degree to which the Bidder's approach to risk management demonstrates: (a) an ability to identify, understand, and minimize or eliminate risk to Canada; (b) how it will lead to a successful implementation of the EPS; (c) thorough analysis of risks that may cause the project to not 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 effectively reduce the probability and impact of risks on the performance of the Contract and increase the reliability of the services provided.

		Assessment of Controllable Risks and Assessment of Non-Controllable Risks. 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 the SOW. 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). **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 relationship between the Bidder's team and Canada.	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 will be effective at building a successful and positive working relationship between the Bidder's team and Canada; (b) that Canada has the authority for managing configuration to the EPS;

		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.	(c) the Bidder's responsibility to Canada and to its own team to provide effective 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 proposed strategy 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 types of Users, to provide support in the use of the EPS and to resolve Users' technical challenges. The Bidder should describe its approach to service desk services to meet the requirements of this solicitation, particularly *section 5.6 – Service Desk* of the SOW, including how it will: i. manage the scalability of the services as the solution responds to the demand for use;	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; (c) ensures adherence to service levels and performance metrics; (d) provides additional operating hours; and (e) manages scalability of the Service Desk services. (f) provides additional value through commitments to additional service levels that will be incorporated into the Service

		ii. categorize, prioritize and log all incidents (e.g. inquiries, issues, service requests); iii. 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, or direct online input by Users) iv. 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; v. identify and describe priorities, response and resolution targets for incidents and service requests that have different impacts; and vi. log, track, manage and report on service desk utilization. vii. provide additional self-help services and support that mitigate the need for Users to contact the service desk.	Level Requirements or through commitments to higher service level performance targets; and (g) provides additional self-help support to Users. (h)
R3.5	Innovation and Value Added	The Bidder should propose innovative ideas and identify any value added offerings that may benefit Canada. If the Bidder can include additional or improved service(s) or	Canada will evaluate the degree to which the Bidder demonstrates:

		functionality(ies) the Bidder should provide an outline of the potential value added. The functionality(ies) and service(s) proposed will be incorporated in the Contract, if they are accepted by Canada. Any functionality and service bid against this criteria must be in compliance with the terms and conditions of the resulting Contract. Should they not be in compliance, they will not be considered by Canada in the evaluation. Any applicable cost for any additional functionality and service must be included as part of the existing Basis of Payment and included in the Bidder's Total Bid Price in Annex 3 – Price Schedule. The price for any functionality and service 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.	(a) additional EPS functionality not included in this solicitation that are of value to modernizing Canada's public procurement practices so that they are simpler, less administratively burdensome and deploy modern comptrollership; (b) additional services that are not included in this solicitation that are of value to modernizing Canada's public procurement practices so that they are simpler, less administratively burdensome and deploy modern comptrollership; (c) an improvement to the timelines identified in this solicitation; (d) the effectiveness in meeting the requirements of the solicitation; (e) the feasibility and that it takes into consideration GC Legislation and Policies; and (f) how it contributes to the overall quality of operations.
R3.6	Product Roadmap	The Bidder should describe its product roadmap strategy for ongoing development of the EPS, including: i. what influences the product roadmap (e.g. competition, market positioning, customer requirements, etc.);	Canada will evaluate the degree to which: (a) the strategy is effectively managed and communicated to the clients; (b) Canada will have the ability to influence the product roadmap(s); and

		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.	(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 milestones as outlined in *section 6.10* of Annex 1 – SOW , including but not limited to: a. management of data and processes in the Bidder's EPS; b. description of supporting technology stack; c. infrastructure management plan; d. system configuration, customization; and e. integration and interoperability plan as the EPS is rolled out.	Canada will evaluate the degree to which the Bidder's technical deployment model demonstrates the following throughout the different milestones as outlined in *section 6.10* of Annex 1 – SOW: (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 current scalability needs (based on existing Government of Canada volumes as outlined in section 1.3 Volumetric Data of Annex 1 - SOW), future scalability needs (based on the expansion to the Broader Public Sector), and performance Service Level Agreements (SLAs) described in this solicitation including through peak periods in business cycles. The description should include, but is not limited to: a) established practices, tools and processes to monitor, track and to manage scalability and performance issues; b) architectural models, features and design that support the proposed solution scalability and performance; and c) examples of expected and unexpected scalability and performance demands and their resolution, based on real-life experiences of Bidder's customer(s) who are of similar size and scope as the EPS.	

		iii. an EPS data management plan that identifies EPS data, meta-data, their format, defaults and describes policies and strategies on data security, access, sharing, storage, and disposition, etc. The Bidder should include a master data plan that describes the solution's master data set, strategies, processes and pre-requisites to interoperate with GC's back-office systems.	
R4.2	Technical Architecture	The Bidder should provide the following 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; ii. a listing of pre-built Application Program Interfaces (APIs) and Web Services that will be used to push and	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 support Canada's system interfaces requirements in this solicitation;

		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; and ii. its approach to disaster recovery that includes an exercise schedule, roles and responsibilities and communication protocol.	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; and (b) the Bidder's approach to disaster recovery and service continuity supports the restoration of the system.
R5	**Security Plan**		
R5.1	IT Security Policies and Procedures (Controls)	The Bidder should demonstrate its ability to comply with the IT security requirements by maintaining policies and procedures that	Canada will evaluate the degree to which the Bidder's response demonstrates thoroughness and effectiveness in achieving the level of security represented by the security

		support IT security throughout the Contract by providing evidence of any existing policies and procedures 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 (f) how it ensures compliance within the organization Note: The Bidder should provide sufficient detail with regard to its policies and procedures in order for Canada to evaluate this response in full.	control families described in *section 1.7* and *Table 1* of *Annex 2—Security and Privacy* of this solicitation and ITSG-33. Canada will evaluate the degree to which the Bidder's response demonstrates effective policy and procedural support for IT Security including technical, operational and maintenance security areas, including the Bidder's anticipated subcontractors where appropriate.
R5.2	IT Security Topology Diagram	The Bidder should provide an IT security topology diagram which should include the following components: i. interfaces - separate bullet for each category	Canada will evaluate the degree to which the Bidder's IT security topology diagram demonstrates that the overall design provides a secure environment.

		ii. web iii. applications iv. databases v. security devices vi. system management vii. backup infrastructure The Bidder should provide one or more of the following, which define information systems components and functions to be separated by boundary protection devices: i. Information system design documentation; ii. Information system architecture.	
R5.3	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 each person, their role & description of their duties, their experience, and certifications.	Canada will evaluate the degree to which the Bidder demonstrates that the security organization: (a) experience of the personnel supporting EPS; (b) roles and the description of the duties of the personnel; (c) relevancy of the current and valid certifications of the personnel in that role; and (d) the plan on how the personnel stay current with security trends.
R5.4	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	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to data segregation: (a) provides logical or physical 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.

		iii. process and procedures to support data segregation .	
R5.5	Disposal and Sanitization	The Bidder should provide its proposed approach to the disposal and sanitization 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; iv. a plan for destruction of duplicate records that may be stored in a records management system or backups; and v. the process it plans to follow when the system is no longer required and is being decommissioned.	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to the disposal and sanitization of Canada's data meets, or effectively mitigates the risk where it does not meet, the requirements for disposal and sanitization of data and IT assets as outlined in *Annex 2 – Security and Privacy* of this solicitation. Canada will evaluate the degree of the strengths, weaknesses and risks of the proposed approach.
R5.6	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 ; ii. Established measures, metrics, and status monitoring and control assessments frequencies;	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; (c) adherence to incident response duties as outlined in Annex 2 – Security and Privacy of the solicitation; and (d) adherence to monitoring requirements outlined in Annex 2 – Security and Privacy of the solicitation.

		iii. Details of data collection 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; and vi. Review and update cycles to support continuous improvement and maturing measurement capabilities.	
R5.7	Industry IT Security Certification	The Bidder should provide proof of its security certification(s) and applicable audit standards for its proposed solution in the form of a copy of a valid certificate or audit standard and describe how the certification or audit standard was assessed and obtained (e.g.: 3rd party, self-assessment) for each IT Security certification and audit standard held, such as: i. FedRAMP; ii. Cloud Security Alliance – STAR; iii. COBIT; iv. ISO 27001; v. PCI DSS; vi. CMM; and	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 this solicitation.

		vii. others. The Bidder should also stipulate if the certification or audit standard applies to the whole solution or to a specified portion of their solution.	
R5.8	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 TBS Standard on Identity and Credential Assurance. The Bidder should identify the level of assurance and demonstrate how it meets the requirements of that level.	Canada will evaluate the degree to which the Bidder demonstrates its solution aligns with the identity and credential assurance requirements defined in Annex 2.

R6	**Additional Functional Requirements** If a Bidder is awarded points for indicating that its EPS will provide the following functionalities and that Bidder is awarded a Contract, the Bidder will be contractually obliged to provide all the functionality it identified as being provided with its EPS in response to *R6 Additional Functional Requirements*. Canada will incorporate these functionalities in the corresponding section of *Part 3 – Functional Requirements of Annex 1 – Statement of Work* in the Resulting Contract.	
R6.1	Additional Functional Requirements – SECTION A - GENERAL	
	In addition to the functionalities identified in Part 3, Section A - General of the SOW, the Bidder should indicate which of the following functionalities it will provide:	
	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 = 3 points
	ii. to support multiple sequential approvals by the same user under a single operation (e.g. batch of approvals).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iii. for Authorized Administrators to configure the default step the workflow returns to when a rejection occurs.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iv. for users, within a group, to assign a workflow step to a single User assigned to that group.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	v. 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 = 3 points

	vi.	to display individual and team procurement workload information in various formats including, but not limited to, tabular, graphs and charts.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	vii.	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 = 3 points
	viii.	for Users to sort, filter and aggregate workload items.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	ix.	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 = 3 points
	x.	for Authorized Users to assign durations to each assigned task, activity, milestone in a project so that procurement team member workload can be determined.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xi.	for Authorized Administrators to configure automatic escalation routines in the event a procurement file sits in queue beyond certain thresholds (e.g. time based).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xii.	to provide Users with a guided or wizard-type process to assist Users in navigating to the right procurement methodology for the goods or services.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xiii.	for Users to reassign the workflow task to another User	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xiv.	to automatically assign a workflow step to an Authorized Administrator and notify the originator in the event that the step identified a group or role no longer available (e.g. no Users	The Bidder cannot provide this functionality = 0 points

		in a group, group renamed).	The Bidder will provide this functionality = 3points
	xv.	for Authorized Administrators 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: Urgency; Required delivery date; and Management instruction.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvi.	for Users, according to their permissions, to view and track workload information such as, but not limited to: Team and individual User workloads across each Department, region, and User; Workload and allocation of the procurement files and documents for each team member; and Scheduled activities, tasks, milestones for each individual User.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvii.	for Users to view all key workload information related to the procurement files in one dashboard including but not limited to: Stage and status of their files; Status of related documents; Status of related activities; Snapshot of their workload; Location of each workload item; and Relevant workload dates. for users to be able to configure and view a dashboard that dynamically displays workload and deliverable information based on their role in EPS.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

		for managers to be able to configure and view a dashboard that dynamically displays key workload and deliverable information on their employees	
R6.2	Additional Functional Requirements – SECTION B PORTAL REQUIREMENTS		
	In addition to the functionalities identified in Part 3, SECTION B PORTAL of the SOW, the Bidder should indicate which of the following functionalities it will provide for these requirements:		
	i.	for Authorized Administrators to create multiple dashboard templates.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	ii.	to automatically control dashboard content based on User role and pre-established business rules.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iii.	for Users to utilize hierarchical operations when displaying data at multiple levels of aggregations such as “drill-down” and “roll-up” operations	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iv.	to support and utilize a variety of visualization models (e.g. charts and graphs).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	v.	to display performance and business information snapshots to Users based on their role.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	vi.	to display a User's actions (to dos) and notifications.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	vii.	for Authorized Administrators to configure publishing cycle times for batch or individual transmission of tender notices to GETS.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	viii.	to automatically set the status and version of the tender notice (e.g. Active, Amended #, Expired, Cancelled, and Awarded).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	ix.	to transmit GETS notices to Users and the public through subscription.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
R6.3	Additional Functional Requirements – SECTION C SOURCING AND CONTRACT MANAGEMENT		
	In addition to the functionalities identified in Part 3, C- Sourcing and Contract Management of the SOW, the Bidder should indicate which of the following functionalities it will provide for these requirements:		
	i.	for the Authorized Administrators 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	ii.	for the Authorized Administrators to create and configure and manage a variety of procurement templates that will assist Authorized Administrators during the planning and strategy development phase.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	iii.	for the Authorized Administrators to configure and manage access to various information sources that are external and internal to the EPS including, but not limited to, relevant policies, rules and regulations (e.g. hyperlink to a policy that resides outside or inside of the EPS).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points

	iv.	for the Authorized Administrators 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 = 3 points
	v.	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 = 3 points
	vi.	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 = 3 points
	vii.	for the Authorized Users 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 = 3 points
	viii.	for the Authorized Users to configure a bidding clock in real time which supports time zones and automatically adjusts for daylight savings time.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	ix.	to display an event countdown clock to show the time remaining for a Sourcing Event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	x.	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 = 3 points
	xi.	To highlight amended sections so suppliers can easily identify changes between versions of the RFx.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points

	xii. to guide Suppliers through the bid submission process (e.g. checklist or wizard).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xiii. to manage a multi-envelope electronic bidding process by allowing Suppliers 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 = 5 points
	xiv. to display a summary of Supplier bids for a final review prior to submission.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	xv. 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 = 5 points
	xvi. to enable Suppliers 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 = 5 points
	xvii. for Suppliers 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 = 3 points
	xviii. to automatically check and validate completeness of the Suppliers' responses.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	xix. 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 = 5 points
	xx. for the Authorized Users 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 = 3 points
	xxi. 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 = 5 points
	xxii. 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. On a group of items; and c. On a whole Basket of Goods.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxiii. for the Authorized Users to configure the technical and financial evaluation to only evaluate certain items in the Catalogue Data 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 = 3 points
	xxiv. for the Authorized Users 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 = 3 points
	xxv. for evaluators to perform scenario analysis prior to and 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 = 3 points
	xxvi. to support Bid Optimization scenario analysis by using various parameters and constraints including, but not limited to:	The Bidder cannot provide this functionality = 0 points

	a. Non-financial criteria; b. Matrices and tiers; and c. Responses to RFx questions.	The Bidder will provide this functionality = 3 points
	xxvii. for the Authorized Users 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 = 3 points
	xxviii. for the Authorized Users 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 = 5 points
	xxix. for the Authorized Users to configure and send notices to Bidders to advise them about outcome of the solicitation process (e.g. Letter of Regret).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	xxx. to link the results of evaluation process to relevant contract award templates such as, but not limited to Letter of Regret and Contract Award Notice.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	xxxi. 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 = 3 points

	xxxii.	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 = 3 points
	xxxiii.	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 in the French version or vice versa.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxiv.	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 = 3 points
	xxxv.	to create, change, store and display procurement and cost related formulas in a repository for re-use during the procurement process (e.g. copy formula from the repository into templates, Contracts, Orders, evaluation sheets, etc.).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxvi.	to look up information entered by the GC User against appropriate central repositories (e.g. UNSPSC Taxonomy).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxvii.	for Authorized Users and GC Users and Suppliers to collaborate on Requisitions.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxviii.	for Authorized Users to create new RFx documents and the resulting contract with user-defined configurable fields: Without templates; From central repository of approved templates; and	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

		Reusing all or parts of previously issued RFx.	
	xxxix.	for Authorized Users to select and insert pre-existing and define new bid evaluation criteria and scoring methodologies in the RFx document.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xl.	for EPS to accommodate complex formulas for technical and financial evaluation scoring.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xli.	for Authorized Users 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlii.	to capture the required information provided by Authorized Users 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xliii.	for Suppliers to submit bid pricing using downloadable spreadsheets e.g. xls).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xliv.	to track status of the Supplier bid (e.g. in progress, submitted, retracted, etc.).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlv.	On bid submission verify integrity and security information stored on the bidder's profile in the Supplier Relationship Management repository meets the requirements specified in	The Bidder cannot provide this functionality = 0 points

	the solicitation.	The Bidder will provide this functionality = 3 points
	xlvi. for Authorized Users to divide the technical bid into sections for evaluation by multiple evaluators and assign to different team members.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlvii. to enable electronic communication between Authorized Users and the bidders to facilitate the exchange of messages and transfer of files, documents etc. (e.g. request for clarification /documentation).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlviii. to export bid evaluation criteria and related weight factors to MS Excel spreadsheet.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlix. to configure the system to ensure the financial part of a proposal is forever locked if the proposal is non-compliant or if the proposal has failed the functional evaluation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	l. for Authorized Users to monitor current bid evaluation status.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	li. to automate the process of moving the resulting contract from the published RFx to a final contract document.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lii. to assign a contract to multiple contracting authorities based on roles.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	liii. for Authorized Users to carry forward and inherit the clauses and conditions from the RFX to the final contract.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	liv. to enable electronic communication and collaboration between Authorized Users and internal/external stakeholders to facilitate the process of collecting, sharing, and validating Supplier related information (e.g. security validation, criminal record checks, etc.).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lv. for Authorized Users to configure, create and monitor contract benchmarks and Key Performance Indicators (KPIs).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lvi. for Authorized Users to re-issue recurring contracts (i.e. contracts requiring renewal).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lvii. for Authorized Users 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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lviii. for Authorized Administrators to configure and build dependencies within process tasks to ensure precursor tasks are completed before beginning others.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lix. for Authorized Administrators to create and manage multiple tasks within a process management tool.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lx. for Authorized Administrators to create and manage electronic	The Bidder cannot provide this functionality = 0 points

		forms that can be embedded into a process management tool.	The Bidder will provide this functionality = 3 points
	lxi.	for Authorized Users to attach documents at the Project and Task level.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxii.	for Authorized Users to include full text and/or reference the clause in solicitation documents.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxiii.	to keep accessible historic content of the clauses and conditions Library.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxiv.	to notify Authorized Users 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxv.	for Authorized Administrators and Authorized Users to create and manage templates (e.g. present Users with a list of standard steps to follow when creating new procurement template).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxvi.	to identify usage and track changes made to a standard procurement template.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxvii.	for Authorized Administrators to configure the process for managing revisions of standard templates and clauses (e.g. rights to create and update clauses and templates).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	lxviii. to enable Authorized Administrators to automatically update templates with the "Active" clauses.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
R6.4	Additional Functional Requirements – SECTION D - PROCUREMENT MANAGEMENT	
	In addition to the functionalities identified in Part 3, D Procurement Management of the SOW, the Bidder should indicate which of the following functionalities it will provide for these requirements:	
	i. for Authorized Users to create an identifier link to indicate items that are equivalent (i.e. same fit, form, and function) to each other.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 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 = 3 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 = 3 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 = 3 points
	v. for Authorized Users 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 = 3 points
	vi. for Authorized Users 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	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	dollar amount).	
	vii. 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 = 3 points
	viii. for Authorized Users 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 provided by the Authorized 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 prior to the issuance of the Catalogue.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 4 points
	ix. for Authorized Users and Suppliers to update the Manufacturer Suggested Retail Price (MSRP), apply the Supplier markup/discount, and display the final price to the User.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 4 points
	x. 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 = 4 points
	xi. for Authorized Users to configure when a User is notified when a Catalogue or Catalogue File has not been updated for a configurable period of time.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xii. to calculate the distance (e.g. air or ground using existing infrastructure, not "as the crow flies") between multiple points used by a predefined formula to determine the overall cost (e.g. number of KMs multiplied by the cost per KM).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xiii. for Users to enter the distance between multiple points which is used by a predefined formula to calculate the overall cost	The Bidder cannot provide this functionality = 0 points

	(e.g. number of KMs multiplied by the cost per KM).	The Bidder will provide this functionality = 3 points
	xiv. 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 = 3 points
	xv. for a cross-PunchOut search for an item.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvi. 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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvii. 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 = 3 points
	xviii. to identify a Shopping Cart Request as either a capital asset or an operating expense based on at least one of the following methods: a. User selection; b. General ledger account; and c. Commodity code.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xix. 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 User.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	xx.	to display products recently viewed by the User.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxi.	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 = 3 points
	xxii.	for Users to share 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 = 3 points
	xxiii.	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 = 3 points
	xxiv.	for Users to view User and Supplier profile information in their shopping carts and orders (e.g. contact details, business address, website URL, etc.)	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxv.	for Authorized Users to configure a Method of Supply to permit Orders to extend delivery date(s)/end date(s) beyond the Method of Supply end date.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvi.	for Authorized Users to manage information about the Method of Supply (e.g. product help, Catalogue background information, help details for the Method of Supply)	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvii.	to support an unlimited number of Catalogues.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	xxviii.	to allow Authorized Users to configure the data fields in a Catalogue that a Supplier can edit within the solution.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxix.	for an Authorized User to configure in a MOS one of the following Payment Methods, in order to utilize during an Order: Supplier Enabled Payment Card (Ghost Card); User Enabled Payment Card (Virtual Card); Other non-credit card payment method	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxx.	for Authorized Administrators to create and manage master unit of measures to be used in the Catalogue (e.g. box, pallet, metric).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxi.	for Authorized Administrators to create and manage master list of Regions and descriptions to be used in the Catalogue.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxii.	for Authorized Administrators to create and manage master list of Methods of Payments (single, monthly, etc.) and Basis of Payment (per diem, ceiling price, fixed price) to be used in the Catalogue.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxiii.	for Authorized Users to create and manage a master list of Catalogue 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 Data File.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxiv.	for Authorized Users to create and manage a Catalogue Data	The Bidder cannot provide this functionality = 0 points

		File using the Master List of Catalogue Attributes.	The Bidder will provide this functionality = 3 points
	xxxv.	to support the creation and management of an unlimited number of line items within a Catalogue.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxvi.	to group items into mandatory bundles where items cannot be removed by the User (e.g. Microsoft Office on a computer).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxvii.	to group together related variants of a specific item according to configurable attributes (e.g. colour, size).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxviii.	for Authorized Users to set the basis of payment from the basis of payment master list when configuring individual line items in a Catalogue Data File.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxix.	for Authorized Users to schedule the frequency (e.g. daily, monthly, on a specific date) to connect to the applicable commodity index feed (e.g. Oil Buyers Guide) in order to update the prices on a dynamic basis in the Catalogue File based on a calculation of markup or discount pricing attribute provided by the Supplier and the commodity index feed marker.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xl.	for Authorized Users to use any version of the Catalogue for a future update.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xli.	for Suppliers to download a locked spreadsheet with editable fields in order to restrict which information can be changed	The Bidder cannot provide this functionality = 0 points

		by the Supplier, and to allow Suppliers to upload the Catalogue changes into the EPS for approval within a secure environment.	The Bidder will provide this functionality = 3 points
	xlii.	for Authorized Users 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xliii.	to apply a pre-defined pricing evaluation framework of the Catalogue Files in a Catalogue and to allow for a review by an Authorized User to ensure that the pricing is in accordance is with the pricing evaluation framework.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xliv.	for Authorized Administrators to configure and schedule business rules that validate Supplier's continued compliance with MOS or Supplier mandatory requirements.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlv.	for Authorized Administrators to create and manage unique Catalogue items to prevent duplication of Catalogue items.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlvi.	to allow a purchase of a good or service for a lower price than what is stated in the Catalogue.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlvii.	for Users to search for a good or service within a specified price range.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	xlviii.	for Users to attach notes and supporting documents.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xlix.	for Users to attach documents to a shopping cart request to be sent to the supplier	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	l.	for users 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	li.	for Authorized Administrators to configure the MOS to provide a supplier list of eligible vendors for the purchase based on business rules and information on the MOS, Catalogue, User Profile, Supplier Profile, Shopping Cart and other related business objects.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lii.	for Users to select an authorized dealer, reseller, or agent when Ordering a good or services (e.g. vehicles).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	liii.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	liv.	to allow comparative shopping in a side by side comparison.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	lv.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lvi.	for Users to identify specific Catalogue items as favourites for future use.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lvii.	for Users to edit a non-catalogue requisition item and replace with an existing Catalogue item(s) and re-route to the applicable workflow.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lviii.	to consolidate shopping carts including the functionality: For Users to manually merge multiple Shopping Carts into one shopping cart For Authorized Users to configure business rules to automatically merge shopping carts For Authorized Users to configure the system to automatically submit Shopping Cart Requests.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lix.	for Authorized Users to configure the default maximum Order response period (in working days) a Supplier has to respond to the Shopping Cart request.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lx.	to allow Users to view a Supplier proposal 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxi.	for Authorized Users to configure business rules for sourcing events under individual Supply Arrangements with respect to	The Bidder cannot provide this functionality = 0 points

	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).	The Bidder will provide this functionality = 3 points
lxii.	for Users to configure a deadline for the submission of a bid according to a Method of Supply business rule.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
lxiii.	for Users to view a list of eligible pre-qualified Suppliers based on sourcing rules under a Supply Arrangement.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
lxiv.	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 (English or French).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
lxv.	for Users to add Suppliers to the invitation for a 2-stage procurement RFx while it is available to be bid on.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
lxvi.	to support a numbering structure that logically relates procurement documents and versions.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
lxvii.	to ensure for any Order, including outstanding Orders, the Order information relates to the appropriate version of the Catalogue File.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
lxviii.	to create multiple Orders from a single Shopping Cart Request based on any data element (e.g. Client, Availability,	The Bidder cannot provide this functionality = 0 points

		Dollar Value), including the functionality to: Send Orders to the appropriate Supplier(s) when there are multiple items associated to a Shopping Cart request from different Suppliers; and Provide the User the option of selecting to create an Order based on the lowest overall cost from a single Supplier or the lowest overall cost from multiple Suppliers in accordance with the applicable MOS and Catalogue Attributes (e.g. Order Thresholds, Minimum Order Quantity).	The Bidder will provide this functionality = 3 points
	lxix.	to allow Suppliers to provide ordering/delivery information once they receive the order (line item status, delivery date, shipping information etc.).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxx.	Authorized Administrator to configure business rules to send copies or a link to the order in EPS to designated stakeholders once it has been ordered.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxi.	for Authorized Users 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxii.	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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxiii.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	lxxiv.	to allow Suppliers to update their bids during the course of the eAuction event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxv.	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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxvi.	to ensure that Suppliers cannot submit a bid after a Reverse eAuction event has closed.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxvii.	for Suppliers to submit questions in relation to a Reverse eAuction event and for the User 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxviii.	for Suppliers during a preview period of a Reverse eAuction 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxix.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxx.	to display an event countdown clock of the time remaining for a Reverse eAuction event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	lxxxi.	to automatically update the Reverse eAuction displayed information without requiring the User to refresh the page.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxii.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxiii.	to allow Users to create, manage, and cancel Reverse eAuction events.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxiv.	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	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxv.	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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxvi.	to allow Users to configure the currency used for a Reverse eAuction event in which a Supplier must submit their bid.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxvii.	to allow Users to configure the bid increment, by a percentage or a dollar amount, for a Reverse eAuction event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	lxxxviii.	to allow Users to configure for an individual Reverse eAuction event the visibility rules for Suppliers to see all	The Bidder cannot provide this functionality = 0 points

		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).	The Bidder will provide this functionality = 3 points
	lxxxix.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xc.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xci.	to allow Users to configure tiebreaker rules for an individual Reverse eAuction event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xcii.	to allow Users to configure whether a floor and/or ceiling price is included in a Reverse eAuction event.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
R6.5	Additional Functional Requirements – SECTION E - SERVICE PROCUREMENT		
	In addition to the functionalities identified in Part 3, E - Service Procurement of the SOW, the Bidder should indicate which of the following functionalities it will provide for these requirements:		
	i.	for Authorized Users 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 = 5 points
	ii.	for Suppliers to indicate if they have a local office in the applicable region within the Catalogue and for Authorized	The Bidder cannot provide this functionality = 0 points

		Administrators to configure when this information is displayed to a User in the ordering process.	The Bidder will provide this functionality = 5 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 = 5 points
	iv.	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. questions and answers form) without the Supplier name being published.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	v.	for Authorized Users 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 = 3 points
	vi.	for 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 = 3 points
	vii.	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 = 3 points
	viii.	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 = 3 points

	ix. to source multiple resources under one SOW with a single Supplier (e.g. both Business Analyst and Project Manager from Supplier A).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	x. to split a SOW for multiple resources into a multi- awarded Supplier contract (e.g. Business Analyst from Supplier A and Project Manager from Supplier B).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xi. 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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xii. 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 = 3 points
	xiii. 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 = 3 points
	xiv. 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 = 5 points
	xv. 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 = 3 points
	xvi. for Users to configure scheduled individual resource performance reviews for the User to complete on a periodic	The Bidder cannot provide this functionality = 0 points

		basis (e.g. every 2 months, at end of Contract only).	The Bidder will provide this functionality = 3 points
	xvii.	for Authorized Users to activate and deactivate resource profiles.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xviii.	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 = 3 points
	xix.	for Authorized Users 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 = 3 points
	xx.	to identify if an individual resource or Supplier has previously done work for the specified organization.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxi.	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 = 3 points
	xxii.	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 = 3 points

	xxiii.	to allow Authorized Users to configure the bidding transparency (e.g. sealed-envelope bidding) for Orders in a Catalogue that require a technical evaluation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxiv.	to allow Authorized Users to configure if Suppliers are allowed to change their status of availability of their services under a Method of Supply, and for the solution to automatically bypass Suppliers who are not available during the Ordering business rules process.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxv.	for Authorized User to create and manage templates that will be used by Suppliers when responding to a shopping cart.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvi.	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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvii.	to evaluate the resource's qualifications against the specific category requirements (e.g. mandatory, point-rated with weightings and with pass marks).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxviii.	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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxix.	for Authorized Users to configure whether the User is required to use a Standard SOW, or is required to create a new SOW.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxx.	to create and manage 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,	The Bidder cannot provide this functionality = 0 points

	deliverables, constraints).	The Bidder will provide this functionality = 3 points
	xxxi. for Users to browse, search, sort, and filter content in the SOW builder.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxii. for Authorized Administrators to configure and manage the sections and related content in the SOW builder by central and/or distributed Authorized Administrators.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxiii. to allow Users to create a new section and applicable content to add to the specific SOW.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxiv. for Users to add additional content to any section within the specific SOW (e.g. content not included in the SOW builder repository).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxv. for Users to browse, search, sort, filter, and select sample SOWs in the SOW library.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxvi. for Users to document and manage individual resource performance and to link the performance to the applicable Supplier.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxvii. to ensure only Authorized Users as part of bidding, ordering, or the contract management process can review an individual's specific and aggregated resource performance.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxviii. to configure a starting performance score for Suppliers without prior Government of Canada performance	The Bidder cannot provide this functionality = 0 points

	evaluations.	The Bidder will provide this functionality = 3 points
	xxxix. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xl. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xli. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
R6.6	Additional Functional Requirements – SECTION G - BUSINESS INTELLIGENCE	
	In addition to the functionalities identified in Part 3, G - Business Intelligence of the SOW, the Bidder should indicate which of the following functionalities 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 = 3 points
	ii. for Users to schedule and automatically generate, print and distribute reports on a predetermined basis defined by the User.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iii. for Users to subscribe and unsubscribe to an automatic report distribution list.	The Bidder cannot provide this functionality = 0 points

		The Bidder will provide this functionality = 3 points
	iv. 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 = 3 points
	v. 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 = 3 points
	vi. to enable Users to build their own custom queries and reports using the EPS'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 = 3 points
	vii. 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 = 3 points
	viii. 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;	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	b. Supplier's delivery performance; and c. service performance.	
	ix. 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 = 3 points
	x. 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 Metadata properties.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xi. to support line item level Business Intelligence and detailed analysis (e.g. 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 = 3 points
	xii. 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 = 3 points
	xiii. to enable and support a broad range of Business Intelligence data visualization tools including, but not limited to:	The Bidder cannot provide this functionality = 0 points

	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 will provide this functionality = 3 points
	xiv. 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 = 3 points
	xv. 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; and c. guided dashboard navigation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvi. 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 = 3 points
	xvii. 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 = 3 points
	xviii. 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 = 3 points
	xix. for Users to discover, view, analyze, report and compare near Near Real-Time data with historical data for all procurement business objects.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xx. 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: Email notification delivery	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxi. to generate and create reports that summarize and calculate various amounts and volumes with totals and sub totals.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxii. for Users to conduct various types of data analysis such as, but not limited to: trend and performance analysis and monitoring; Supplier fragmentation analysis; Forecasting; Deleted Deleted Deleted Deleted Deleted Deleted	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	xxiii. 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: Calculated savings and expenditures by various factors; Purchases by various factors; Usage of selected clauses from the clause library; and Award of contracts by various factors.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxiv. to allow for variance analysis in dollars, percentages, time (e.g delta between any sums, variance based on time such as hours/days and/or dates).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
R6.7	Additional Functional Requirements – SECTION H - SUPPLIER RELATIONSHIP MANAGEMENT	
	In addition to the functionalities identified in Part 3, H - Supplier Relationship Management of the SOW, the Bidder should indicate which of the following functionalities 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 = 5 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 = 5 points
	iii. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	iv. 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 = 5 points
	v. for authorized administrators to configure and schedule survey.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 7 points

	vi. 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 = 10 points
	vii. 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 = 10 points
	viii. 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 = 3 points
	ix. 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 = 10 points
	x. 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 = 10 points
	xi. to route scorecards for review by identified Users.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 10 points
	xii. 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 = 10 points
	xiii. 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 = 5 points

	xiv. to import and export qualitative and quantitative data from both third party sources and from within the EPS as part of scorecard generation.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	xv. 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 = 5 points
	xvi. 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 = 5 points
	xvii. to allow survey creator and respondents to save partially built and 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 = 5 points
	xviii. 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 = 5 points
	xix. to allow survey creator and respondents to upload, download, send and receive multiple attachments to survey.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points

	xx. 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 = 5 points
	xxi. 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 = 5 points
	xxii. 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 = 5 points
	xxiii. to track and automatically notify Authorized Users 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 (e.g. active or inactive based on a set of configurable rules).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 5 points
	xxiv. 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 = 3 points

	xxv. for Authorized Administrators to create and configure an intelligent Supplier self-registration form with optional, mandatory fields that will prompt the Supplier for further information and documents based on combinations of configurable business rules and provided information.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvi. for Authorized User to validate and approve information and certificates provided by the Supplier, including, but not limited to: Professional certifications; Insurance policies; Security clearances; and Financial statements.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvii. to pull information from Supplier's response to a sourcing event into its Supplier profile.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxviii. to pull and share Supplier information and data in Near Real-Time from third party content providers and systems (e.g. CRA) such as but not limited to supplier legal name and CRA business number.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
R6.8	Additional Functional Requirements – SECTION I – DATA AND INFORMATION MANAGEMENT	
	In addition to the functionalities identified in Part 3, I – Data and Information Management of the SOW, the Bidder should indicate which of the following functionalities it will provide for these requirements:	
	i. to automatically monitor the quality of information (transactional and master data repositories) by evaluating the following dimensions: completeness, conformity, consistency, accuracy, duplication and integrity.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	ii. to measure and assess data quality by applying system and user-configurable scenarios, business-system rules and schedules, in various situations such as: a. Upload of new Catalogue items; b. Import of updated/new classification code schemes; c. Data synchronisation checks between EPS and SAP; and d. Transactional and master data scheduled verifications.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iii. to prepare and disseminate the results of data quality verifications to Users in summarized or detailed forms.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	iv. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	v. 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)).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	vi. 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,	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	integrity constraints or other GC business rules that define sufficient data quality for the organization.	
	vii. to create and manage manually and automatically master data as per recognized and approved by 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	viii. 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 user-defined product codes (e.g. UNSPC).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	ix. to offer Supplier data enrichment capabilities regarding data elements, such as,: Parent/child relationships; and Standard Industrial Codes (SIC).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	x. to ensure consistent classification of similar items from different data sources using automatic and rule-based classification.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xi. to allow record, and where applicable, group of records, to be classified in accordance with the organisation's records classification scheme.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xii. to support close linkage and interaction between records classification and other records management processes, such as capture, access and security, disposition, searching and retrieval,	The Bidder cannot provide this functionality = 0 points

	and reporting.	The Bidder will provide this functionality = 3 points
	xiii. for the creation and management of bookmarks/favorites to link to a specific page within EPS.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xiv. for the validation of text fields using editing tools, such as autocorrect or spellchecker for the appropriate official language.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xv. 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).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvi. to enable versioning for individual or group of records, including features such as, version numbering and the ability to revert a document to a previous revision.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xvii. to enable Near Real-Time collaboration on a procurement file and associated documents using features, such as document versioning, document locking or conflict resolution in multiuser environments.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xviii. for the configuration, execution and tracking of record imports from external source.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xix. to capture all User documents, information, and records and retain them in the EPS.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

	xx. to configure the naming of electronic records through manual (User input) and automated processes.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxi. for the tracking of all disposition actions carried out on electronic records (migration, import, export).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxii. to report the details and outcome of any migration process to ensure the integrity of electronic records.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxiii. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxiv. for disposition classes to be systematically or manually applied to existing, received or newly created records and associated Metadata, and where applicable, group of records.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxv. to make the entire content of a record or group of records available to reviewers, subject to applicable access restrictions.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxvi. for Authorized Administrators to create and manage taxonomies of different types (e.g. lists, synonyms, hierarchies (e.g. UNSPSC), faceted navigation and thesaurus, ontologies), such	The Bidder cannot provide this functionality = 0 points

	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)); Deleted Deleted	The Bidder will provide this functionality = 3 points
	xxvii. for Authorized Administrators to expand the definition of data elements by adding and configuring custom data attributes (e.g. security, rights and public availability properties).	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxviii. to configure and restrict the ability to amend record Metadata during the lifecycle of record based on business rules defined by GC.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxix. for the capture of Metadata entered manually by a User.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxx. to enable user-defined Metadata fields for the entry of descriptive information about the record.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points
	xxxi. 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.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

R6.9	Additional Functional Requirements – SECTION J – USER MANAGEMENT	
	In addition to the functionalities identified in Part 3, J – User Management of the SOW, the Bidder should indicate which of the following functionalities it will provide for these requirements:	
	i. to make registration remain incomplete (preventing access to certain solution functionality) until User account configuration is complete.	The Bidder cannot provide this functionality = 0 points The Bidder will provide this functionality = 3 points

ATTACHMENT 3 TO PART 4:

PROOF OF PROPOSAL

(PoP) TEST

ATTACHMENT 3 TO PART 4: PROOF OF PROPOSAL (PoP)TEST

1. POP TEST METHODOLOGY

The purpose of the PoP Test is to test compliance of the Bidder's proposed solution against a sample of the requirements of this bid solicitation. The PoP Test will consist of the Bidder's demonstration of specific tasks pertaining to a selection of requirements as described in Annex 1 – Statement of Work (SOW). The following table outlines the requirements and associated tasks that must be demonstrated by the Bidder in the PoP Test. The Bidder is permitted to demonstrate the tasks in any order it chooses but must demonstrate all tasks within the allocated time to successfully pass the PoP Test

2. REQUIREMENTS

SOW NUM	Requirement	Tasks that must be demonstrated by the Bidder to successfully pass the POP Test
A-02.01	search based on reportable fields, document attributes and Metadata.	1. Performing a federated search for catalogue items across multiple catalogues. 2. Filtering search results using price ranges. 3. Exporting search results to a CSV file.
A-03.01	for Authorized Administrators to configure existing business artifacts and attributes, create new artifacts and attributes and control business behaviour (such as conditions that must be met before user can amend an order) using business rules. Specifically, they must be able to i. add new attributes or modify functionality of existing attributes, ii. Set attribute type (number, free text, money, pick list, Boolean, uploaded attachment/document, look up, etc.) iii. Set attribute GUI position and tab order iv. Set attribute level behaviour and properties (labels, mouse over help, mandatory/optional, visibility, default value, etc.) v. Create business and validation rules vi. Set print layout vii. Specify which attributes are internal to EPS and which ones will be shared with the supplier (in RFX, Order, etc.)	4. Adding a new free text field to a shopping cart request and demonstrate the following field level functionality: a. set label; b. set a default value; and c. set the field as mandatory or optional. 5. Adding a new date field to a shopping cart request. 6. Adding a new attachment field to a supplier profile. 7. Creating and applying validation rules on a shopping cart request. 8. Adding new fields to the order print layout.

	viii. Specify which data attributes are pre-populated when the artifact is created (such as prepopulate user data from the requester's user profile on a requisition when a requisition is created) ix. Specify which data attributes are carried forward to related business artifacts in a process (example – creating orders from shopping carts) x. Specify which attributes are included when the Business artifact is copied. xi. Specify the behaviour (business rules, validation rules, etc.) that apply when the business artifact is modified.	
A-10.01	for Authorized Administrator to create, configure and manage automated workflow approval process templates for each business artifact (such as requisitions, RFXs, supplier profile, user profile, etc.). Authorized Administrators must be able to configure workflow approval process templates based on system data, business rules, and groups/roles/permissions. For each workflow stop, the Authorized Administrators must be able to configure: i. the sequence (position of this stop versus other stops); ii. whether it is sequential or parallel; iii. who it is assigned to (group or individual); iv. the action required (watcher only, approve/deny or edit/approve/deny); v. list of acceptable reasons for approving or denying; vi. escalation rules (length of time dormant, group or individual to escalate to).	9. A User creating a workflow approval process or an RFx which includes the following: a. two or more sequential stops and at least one parallel stop; b. stops for watchers only, approval/deny and edit/approval/ deny; c. denying a request; d. approving a request; e. stops assigned to an individual; f. stops assigned to a group; g. escalation rules.
A-10.04	for users 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).	10. Users manually adding workflow stops.
A-10.15	to enable the use of a graphical or textual tool for creating and configuring workflows and testing.	11. A User creating and testing a workflow approval process for a supplier profile.
A-11.02	for Authorized Users to configure business rules for automatic assignment of requisitions to groups or individual members of a procurement team.	12. Configuring a business rule to assign a requisition to an individual User based on the commodity specified on the file.

A-11.03	for Authorized Users to manage team members participating in the sourcing event.	13. Assigning team members to a sourcing event.
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.	14. An Authorized Administrator configuring a dashboard template.
B-03.06	for Users to organize their dashboard.	15. A User organizing their dashboard (based on the templates created in B-03.01) and adding a contract spend report.
B-04.06	to communicate to all Users or a subset of Users (e.g. at a minimum, being able to create e-mail distribution lists).	16. A User creating an e-mail distribution list for all acquisition card holders in the system.
C-01.11	for GC Users to assign multiple financial codes to a Requisition line item.	17. A User creating a requisition with 3 line items and assigning a different financial code to each one.
C-01.15	to track requisitions throughout the procurement process.	18. Tracking a line item from the catalogue to the requisition, order, goods receipt and settlement.
C-03.03	for Authorized Users to search central repositories for various artefacts and templates during RFx creation.	19. Searching for a clause in the clause library and adding the clause to a draft contract as part of the creation of an RFx. 20. Searching for a RFx template and creating an RFx based on the template. 21. Searching for a contract template and creating a contract based on the template.
C-04.02	for Authorized Users to create and manage reusable source lists.	22. Creating a source list of suppliers based on a commodity code.
C-05.01	for Suppliers to complete and submit electronic bids.	23. A supplier completing and submitting an electronic bid submission form to a solicitation that must contain at least: a. one mandatory custom field; and b. one optional custom field.
C-05.04	to allow Authorized user to manually enter bid submissions received outside EPS and set the submitted date and time of each submission.	24. Manually entering bid submissions received outside of EPS.

		25. Automatically tracking date and time of a submission.
C-05.05	to generate an official record (e.g. electronic receipt) for both on-line and off-line bid submissions.	26. Creating an official record for an online bid submission and an off-line bid submission.
C-05.06	for Suppliers to retract submitted bids and resubmit final bid prior to bid closing time.	27. A supplier retracting and resubmitting an electronic bid.
C-06.02	for Authorized Users to access bid submissions after bid closing	28. Accessing a bid submission after bid closing. 29. Restricting access to bid submissions before bid closing.
C-06.04	for Users to document their evaluation results using pre-configured evaluation grids with embedded formulas.	30. Setting up evaluation grids with embedded formulas. 31. Assigning evaluation grids to Users. 32. Evaluating bids using evaluation grids.
C-06.07	to enable and support individual and consensus team evaluation processes.	33. Managing individual and team consensus evaluation processes.
C-06.11	to calculate the final bid score based on RFx defined formulas and selection methodology.	34. Calculating the final bid score based on evaluation and selection methodology.
C-07.02	for Authorized Users to award contracts.	35. Awarding a contract to a bidder after successfully wining a competitive process with at least 3 vendor proposals where: a. One of the vendor proposals is non- compliant (does not meet mandatories); and b. The other vendor proposals are compliant but scored lower in the evaluation than the winning bidder.
C-07.07	for Authorized Users to configure contracting attributes (e.g. contract start date / end date, option period(s), optional services, contract limits and tolerance levels).	36. Configuring contract attributes (start date, end date, option periods, and contract limits).
C-08.06	for Authorized Users to create, approve, manage and control contract amendments.	37. Creating and approving a contract amendment.
C-10.01	for Authorized Administrators to create and manage a clause repository (library) in both official languages that can be accessed by Authorized User to create RFx, RFx amendments, Contracts, and contract	38. Creating a clause library with at least 3 clauses in both official languages.

	amendments.	
C-10.02	for Authorized Administrators to identify corporate and custom clauses and designate clauses that require a workflow to be modified.	39. Designating a clause that must be workflowed for approval if it is modified. 40. Creating the workflow rule to route the modified clause to a contracting manager for approval. 41. A User editing the clause. 42. Routing the clause to the manager for approval. 43. Manager approving the clause. 44. Showing the history of the change.
D-01.01	For Authorized Administrators to configure and manage catalogues. They must be able to: i. add new fields and set field type (number, free text, pick list, Boolean, uploaded attachment/document, etc) ii. set business and validation rules iii. Set field level behaviour (labels, mouse over help, mandatory/optional, visibility, default value, etc) iv. Set GUI and print layout v. Specify which fields are internal to EPS and which ones will be shared with the supplier (on requisitions and orders.) vi. Specify which data attributes are pre-populated when the catalogue or catalogue line item is created vii. Specify which fields are copied to the shopping cart when a line item is added to the shopping cart	45. Add a new field to a catalogue. 46. Loading new data into the catalogue field. 47. Searching for items using the new field. 48. Displaying new field in the catalogue line item details. 49. Copying the new field to the shopping cart.
D-02.04	to export Catalogues into different Catalogue Data File formats in order to allow an Authorized User to work off-line in the Catalogue Data File and to import it back into EPS.	50. Exporting a catalogue in XLS format. 51. Editing the exported file. 52. Importing the file back into the EPS.
D-03.02	for Authorized Users to create the configuration options (e.g. hard drive size for a computer) for a configurable Catalogue item (e.g. Computers, Vehicles) to be selected by the User in the Shopping Cart.	53. Creating a catalogue that contains options that must be chosen by the User once the item has been selected.
D-03.14	for Authorized Users 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	54. Ensuring that a User cannot place an additional Order once the cumulative limitation has been met

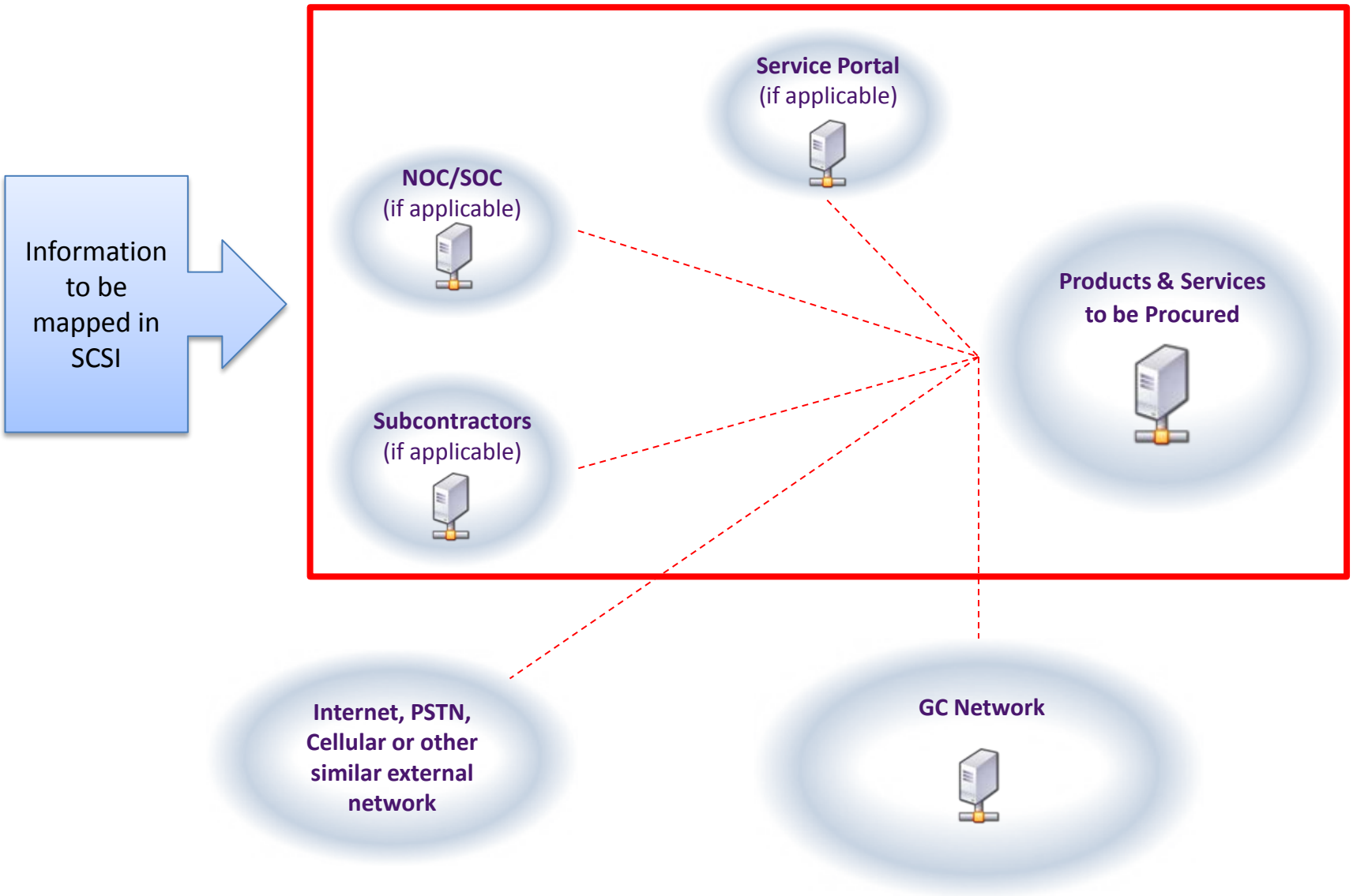
	Orders issued reaches the applicable threshold.	on the Method of Supply.
D-06.05	for Authorized Users to configure and manage tiered pricing for items on each Catalogue that are used to determine pricing on an individual shopping cart.	55. A User configuring tiered pricing on a catalogue.
D-08.04	to compare Catalogue items according to their specifications (e.g. price, size, weight, benchmark evaluation).	56. Comparing two or more catalogue items.
D-09.06	for Users to navigate Catalogue content via a category driven hierarchy.	57. Navigating catalogue content using commodity categories.
D-12.05	for Users to save the Shopping Cart for later retrieval.	58. Saving and re-opening a shopping cart request.
D-14.02	for Suppliers to withdraw a proposal to a Shopping Cart request up to the time of Order issuance.	59. Withdrawing a proposal to a shopping cart request.
E-02.03	to allow Authorized Users to set fixed prices, ceiling prices, and rates for geographical areas and individual categories and sub-categories for all Suppliers or to set individual prices for individual Suppliers. to allow Authorized Users to set fixed prices, ceiling prices, and rates for geographical areas and individual categories and sub-categories for all Suppliers or to set individual prices for individual Suppliers.	60. Setting a ceiling price for the service. 61. Allowing the supplier to enter a price lower than the ceiling price. 62. Accepting the new price. 63. Completing the request/order.
E-08.01	to configure and manage a library of sample SOWs by central and/or Authorized Administrators.	64. Creating and editing a Statement of Work in a library.
G-01.01	to configure, add, delete and modify fields in reports.	65. Adding a new field to an existing report.
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: i. Purchasing orders; ii. Requisitions; iii. Catalogue items; iv. Contracts; v. Sourcing projects; and vi. Suppliers.	66. Reports for purchase orders, contracts and sourcing projects.
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: i. MS Excel/MS Word; ii. CSV file; iii. XML file; and iv. PDF.	67. Exporting a purchase order report to MS Excel and PDF.

H-01.09	to enable Supplier to set up their interests for a single or multiple commodities (e.g. by commodity code, by service offering, by region).	68. A supplier indicating an interest in their profile for commodities based on the UNSPSC taxonomy.
H-01.10	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: i. Import and attach electronics copies of their qualifications certifications in multiple formats (e.g., PDF, .PPT, .BMP, .GIF, .JPEG, .JPG); and ii. Enter and update validity period of qualifications and certifications (e.g. expiry dates).	69. Loading a new certificate (PDF) to a supplier profile.
H-02.02	for Authorized Users to add notes on Supplier performance	70. Adding notes to a supplier profile.
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.	71. Tracking, measuring and reporting on performance progress for a supplier.
H-02.04	for Authorized Users to access Supplier performance evaluation history information and data at any time including but not limited to: i. During the RFx evaluation; ii. During Contract Management; and iii. During procurement File Close-Out.	72. Accessing a supplier's performance evaluation history during an RFx evaluation.
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.	73. Configuring a scheduled task to export a report on suppliers that contains at least one custom field.
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.	74. Creating a procurement checklist that includes at least one free text field, checkbox and drop down list.
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.	75. Preventing a user from ordering off a catalogue based on the user's role.
J-01.11	for Authorized Administrators to delegate their own role to another User for a configurable period of time.	76. Delegating a role to another user for a configurable period of time.

ATTACHMENT 4 TO PART 4:

SUPPLY CHAIN SCOPE DIAGRAM

Supply Chain Network Diagram



ATTACHMENT 1 TO PART 6: Service Level Agreements – Security & Privacy

ATTACHMENT 1 TO PART 6 – Service Level Agreements - Security & Privacy

1. Service Level Agreements

Third party sub-contractors may be used in fulfilling the contract requirements as defined by the RFP and the SOW. Table 1 below identifies key Security and Privacy areas that will assist the Contractor in negotiating Service Level Agreement with its third party. In order for the GC to have visibility into the proposed solution, these key areas have been identified as guidance only to the Contractor for consideration in their sub-agreements through the proposed solution supply chain (i.e. with partners or sub- contractors). GC will only assess its security and privacy areas against Annex 2 requirements within the RFP.

Table 1 describes the Service Level Agreements for guidance only.

Category	Sub-Category	Description
Service Continuity	Contingency Planning	The Contractor should perform backup, recovery and refresh operations on a periodic basis. The Contractor should provide Recovery Point Objective, RPO (=4 hours) and Recovery Time Objective, RTO (= 72 Hours) as part of the Service Levels. The Contractor should, at a frequency that is consistent with RTO/RPO: a) Conduct backups of user-level information; b) Conduct backups of system-level information; c) Conduct backups of documentation including security-related documentation; and d) Protect the confidentiality and integrity of backup e) information at the storage location in accordance with media protection requirements.
Security Operations	Configuration Management	The Contractor should develop, document, and maintain under configuration control, a current baseline configuration.
Security Operations	Configuration Management	The Contractor should develop, document, and maintain an inventory of the 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; and e) Is updated as an integral part of component installations, removals, and services.
Security Operations	Configuration Management	The Contractor should manage configuration settings for 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.

Category	Sub-Category	Description
Security Operations	Security Monitoring	The Contractor should automatically monitor on a continuous basis events to: a) Detect attacks, Incidents and abnormal events against the Hosting Environment; b) Identify unauthorized use and access of Data and components; and. c) Respond, contain, and recover from threats and attacks.
Security Operations	Security Monitoring	The Contractor should respond to security alerts, advisories, and directives from designated external organizations 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; c) Disseminating security alerts, advisories, and directives to Operators with security responsibilities; and d) Implementing security directives, or notifies the vendor regarding the degree of non-compliance.
Security Operations	Security Incident Management	The Contractor should notify via phone and email (7 days x 24 hours x 365 days), based on priority, of any suspected or actual Security Incidents, including: 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.
Security Operations	Security Incident Management	The Contractor should report all suspected or actual privacy and security violations as Security Incidents.
Security Operations	Security Incident Management	The Contractor should provide all evidence associated with a Security Incident that includes: a) Results of historical logs and audit records research associated with one or many Partners; b) Results of analysis of logs and audit records associated with one or many Partners; c) Logs and audit records; and d) Additional information or data.

Security Operations	Security Incident Management	The Contractor should provide Security Incident post-mortem reports, within 72 hours of a request, 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; and i) Limitations/issues.
Security Operations	Investigations	The Contractor should implement an audit and investigation process that allows only specific, pre-authorized representatives to request and receive discrete access and information associated with Data (user data, event logs, content) for the purposes of conducting investigations. The Contractor shall not disclose such access to End Users. The Contractor shall report such access on a monthly basis by Partner organization.
Security Operations	Security Reports	The Contractor should provide summary reports and statistical logs periodically (i.e. weekly, monthly or quarterly) and on-demand including: a) Dashboard reporting on system performance b) Real-time and historical performance against SLA c) Reporting on Utilization Statistics d) Security incident reports, post-mortem, adhoc reports, and associated evidence; e) Security Incident tickets; f) User activity reports; g) Operator activity reports; h) Access reports; i) Configuration audit reports; j) Configuration change reports; k) File integrity monitoring reports; l) Inventory reports; m) Vulnerability reports; n) Security threat reports; o) Emergency Request For Changes and Request For Changes; and p) Patches and security patches implemented.

Category	Sub-Category	Description
Security Operations	Patch Management	The Contractor should perform patch management appropriate to the scope of their control this 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; c) Prioritizing critical patches and service packs using a risk-based approach; d) Taking applications offline and bringing them back online; e) Aligning criticality levels for patches; 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
Security Policy Compliance Monitoring	Vulnerability Management	The Contractor should: a) Report any security issues immediately upon learning of their existence; b) Track identified security issues; and c) Report progress until each security issue is fixed or mitigated.
Planning	System Security Plan	Within 45 days after contract award, the Contractor should provide a System Security Plan (SSP). The Contractor should develop a security plan for the information system that: a) Is consistent with the Contractor's enterprise architecture; b) Explicitly defines the authorization boundary for the system; c) Describes the operational environment; d) Describes the policies and associated requirements for all components; e) Describes relationships with or connections to other information systems; f) Provides an overview of the security control requirements for the system; g) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and h) Is reviewed and approved prior to plan implementation. The Contractor should review the security plan for the information system on an annual basis. The Contractor should update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Category	Sub-Category	Description
Risk Management	Authorization Maintenance	The Contractor should maintain the security authorization state through continuous monitoring and annual audit of the implemented security requirements to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the operational environment. The Contractor should provide evidence to support authorization maintenance activities, within 30 days, following all changes to the Infrastructure within the Contractor's control. The Contractor should update security operating procedures as part of authorization maintenance within 30 days of a request.
Risk Management	Security Assessments - Independent Assessment	The Contractor should employ an independent assessor or assessment team to conduct an assessment of the security controls in the information system.
Risk Management	Security Assessment - Plan of Action and Milestones	The Contractor should develop a plan of action and milestones for the information system to document the Contractor's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. The Contractor shall update the existing plan of action and milestones on a quarterly basis, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
Risk Management	Continuous Monitoring	The Contractor should ensure and demonstrate that the security posture of the 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.
Data Security	Data Protection	The Contractor should ensure all data centres and data warehouses meet industry standard Data Protection Certification and Accreditation (including PCI compliance) in accordance with the data protection requirements in this RFP.
Data Security	Data Protection	The Contractor should ensure that the integrity and confidentiality of the data is protected using cryptographic solutions unless otherwise protected by approved alternative mechanisms.
Data Security	Data Loss Prevention	The Contractor should implement security mechanisms to prevent data leakage.

Category	Sub-Category	Description
Network and Communication Security	Encryption	The Federal Information Processing Standard (FIPS) 140-2 specifies the security requirements that should be satisfied by a cryptographic module utilized within a security system, sub-system, or component protecting protected information. Prior to using any cryptographic module, the contractor shall provide a copy of the relevant FIPS 140-2 validation certificate as evidence of FIPS 140-2 validation, or, as a minimum, the validation certificate number.
Network and Communication Security	Boundary Protection and Zoning	The Contractor should monitor and analyze network traffic, in real time, to detect attacks and evidence of compromised Infrastructure components. Specifically, the Service Infrastructure should monitor and control communications at the external boundary of the system and at key internal boundaries within the system. The Contractor should 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.
Network and Communication Security	DNS	Should be configurable to use DNSSEC for DNS queries.
Security Policy Compliance Monitoring	Malware Protection	The Contractor should implement and maintain network protection capabilities to detect and eliminate malicious software and/or unauthorized external connection attempts on network monitoring devices, servers, peripheral devices, and desktop workstations. All data should be scanned for the presence of malware. There should be an active host- protection mechanisms on servers that are actively scanning malware at a frequency greater than once a month.
Security Operations	Logging and Auditing	Provide the ability to track system and detailed user activity and capture events and audit logs to a centralized audit log system. The audit log system should: a) Include centralized and time-synchronized logging of allowed and blocked activities with 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; and d) Store logs for at least 6 months.

Category	Sub-Category	Description
Security Operations	Logging and Auditing	Audit records should include: a) What type of audit event occurred; b) When (date and time) the audit event occurred; c) Where the audit event occurred; d) The audit source of the event; e) The outcome (success or failure) of the audit event; and f) The identity of any user/subject associated with the audit event.
Security Operations	Logging and Auditing	The Contractor should implement an audit review process that includes: a) Review and analysis of audit records annually and within 20 working days of a request for indications of inappropriate or unusual activity; b) Report findings of the audit review process within 10 working days of completion of the audit; and c) Adjust the level of audit review, analysis, and reporting when there is a change in risk or as requested.
Security Operations	Security Incident Management	The Contractor, for Security Incidents tickets, should include 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 and description of attack/event; g) Whether attack appears to have been successful and impact; h) Attack scope (to an organization and/or across many organizations); i) Estimated number of systems affected by organization; j) List of systems affected by organization; k) Apparent source/origin of attack/Incident/event; l) Date/time of attack/Incident/event; m) Estimated injury level /sector; n) Estimated impact level; o) Attack/Incident/event duration; p) Actions taken; q) Status of mitigations; and r) Applicable logs or evidence data
Security Operations	Security Incident Management	The Contractor should include a technical solution (for example, a web-application firewall) that detects and prevents web-based attacks (e.g. injection flaws, buffer overflows, cross-site scripting, etc.) in front of public-facing web applications.

Category	Sub-Category	Description
Personnel Security	Personnel Screening	a) The Contractor should screen individuals prior to authorizing access to the information system. b) The Contractor should rescreen individuals according to conditions requiring rescreening. c) For Foreign Contractors, see Part 6, 6.1(a) – Security and Privacy Requirements for Foreign Suppliers (Personnel Screening).
Personnel Security	Personnel Termination	a) The Contractor, upon termination of individual employment, should terminate information system access. b) The Contractor, upon termination of individual employment, should retrieve all security-related organizational information system-related property.
Personnel Security	Access Agreements	The Contractor should ensure that access to information with special protection measures is granted only to individuals who: (a) Satisfy associated personnel security criteria; and (b) Have read, understood, and signed a nondisclosure agreement.
Personnel Security	Third-Party Personnel Security	The Contractor should satisfy the personnel security control requirements including security roles and responsibilities for third-party providers. The Contractor should ensure security screening of private sector organizations and individuals who have access to Protected information and assets.

Category	Sub-Category	Description
System Security	System Security Plan	The Contractor should provide a System Security Plan (SSP). The Contractor should develop a system security plan for the information system that: a) Is consistent with the Contractor's enterprise architecture; b) Explicitly defines the authorization boundary for the system; c) Describes the operational environment for the EPS; d) Describes the policies and associated requirements for EPS components; e) Describes relationships with or connections to other information systems; f) Provides an overview of the security control requirements for the system; g) Provides the process of continuous monitoring that ensures adherence to this plan; h) For the SA&A Gating process (gate 1, 2 and 3), describe the IT security implementation plan for each SA&A gate; i) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and j) Is reviewed and approved by the GC prior to plan implementation. The Contractor should review the security plan for the information system on an annual basis. The Contractor should update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments
Privacy Breach Response	Privacy Breach Response	For each Contractor involved in delivering the required services, the Contractor should deliver a final Privacy Breach Protocol within 90 days of Contract award that is approved by the Project Authority as part of their incident management processes for the handling of any privacy related incidents. The privacy breach should also be described, which should include details on how any privacy breaches will be identified, reported and mitigated. The Contractor should notify the Contracting Authority immediately of any security or privacy breaches.

FORM 1 TO PART 4:

RFP SUBMISSION FORM

Table 1 - 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. 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:

Table 2 - Declaration of Convicted Offences

As applicable, pursuant to subsection Declaration of Convicted Offences of section 01 of the Standard Instructions, the Bidder must provide, precedent to Contract award, a completed Declaration Form (www.tpsgc-pwgsc.gc.ca/ci-if/formulaire-form- eng.html), to be given further consideration in the procurement process.

This declaration form must be submitted as part of the bidding process. Please complete and submit in a **sealed envelope labelled "Protected**" to the attention of Integrity, Departmental Oversight Branch, PWGSC, 11 Laurier Street, Place du Portage, Phase III, Tower A, 10A1, Room 108, Gatineau (Quebec) Canada K1A 0S5. Include the sealed envelope with your bid submission. This form is considered "Protected B" when completed.	
Complete Legal Name of Company:	
Company's address:	
Company's Procurement Business Number (PBN):	
Bid Number:	
Date of Bid: (YY-MM-DD)	

Have you ever, as the bidder, your affiliates or as one of your directors, been convicted or have pleaded guilty of an offence in Canada or similar offence elsewhere under any of the following provisions [1] :			
	Yes	**No**	**Comments**
Financial Administration Act 80(1) d): False entry, certificate or return 80(2): Fraud against Her Majesty 154.01: Fraud against Her Majesty **Criminal Code** 121: Frauds on the government and contractor subscribing to election fund 124: Selling or Purchasing Office 380: Fraud – committed against Her Majesty 418: Selling defective stores to Her Majesty	☐ ☐	☐ ☐	
In the last 3 years, have you, as the bidder, your affiliates or one of your directors, been convicted or have pleaded guilty of an offence in Canada or elsewhere under any of the following provisions [1]:			
Criminal Code 119: Bribery of judicial officers 120: Bribery of officers 346: Extortion 366 to 368: Forgery and other offences resembling forgery 382: Fraudulent manipulation of stock exchange transactions 382.1: Prohibited insider trading 397: Falsification of books and documents 422: Criminal breach of Contract 426: Secret commissions 462.31 Laundering proceeds of crime 467.11 to 467.13: Participation in activities of criminal organization **Competition Act** 45: Conspiracies, agreements or arrangements between competitors 46: Foreign directives 47: Bid rigging	☐ ☐	☐ ☐	

49: Agreements or arrangements of federal financial institutions			

[1] for which no pardon or equivalent has been received.

	Yes	No	Comments
52: False or misleading representation 53: deceptive notice of winning a prize			
Corruption of Foreign Public Officials Act 3: Bribing a foreign public official 4: Accounting 5: Offence committed outside Canada **Controlled Drugs and Substance Act** 5: Trafficking in substance 6: Importing and exporting 7: Production of substance	☐ ☐	☐ ☐	
Other Acts 239: False or deceptive statements of the Income Tax Act 327: False or deceptive statements of the Excise Tax Act	☐	☐	
Lobbying Act Registration of Lobbyists 5: Consultant Lobbyists 7: In-house Lobbyists (Corporations and Organizations)	☐	☐	

Additional Comment

☐ I, (name)_____, (position)_____, of (company name bidder)

_____ _____authorise PWGSC to collect and use the information provided, in additional to any other information that may be required to make a determination of ineligibility and to publicly disseminate the results.

☐ I, (name) _____, (position) _____, of (company name bidder)

_____certify that the information provided in this form is, to the best of my knowledge, true and complete. Moreover, I am aware that any erroneous or missing information could result in the cancellation of my bid as well as a determination of ineligibility/suspension.

We appreciate your interest in doing business with The Government of Canada and your understanding on the additional steps that we need to take to protect the integrity of PWGSC's procurement process.

Table 3 – Integrity Provisions

In accordance with Article 5.1.1 under Part 5, please complete the Form below.

Complete Legal Name of Company	
Company's address	
Company's Procurement Business Number (PBN)	
Solicitation number	
Board of Directors (Use Format – first name last name) Or put the list as an attachment	
1. Director	
2. Director	
3. Director	
4. Director	
5. Director	
6. Director	
7. Director	
8. Director	
9. Director	
10. Director	
Other members	
Comments	

Table 4: Former Public Servant

<table>
<tr><td rowspan="4">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 FPS, bidders must provide in writing before contract award for each question below, the answer and, as applicable, the information required.

If the Contracting Authority has not received the answer to the question and, as applicable, the information required by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the answer and, as applicable, the information required. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

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.

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.</td><td colspan="2">Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation?

Yes ☐ No ☐

If yes, provide the following information:</td></tr>
<tr><td>a. name of former public servant;</td><td></td></tr>
<tr><td>b. name of former public servant:</td><td></td></tr>
</table>

Table 5 – Work Force Adjustment

Work Force Adjustment Directive See Table 4 for a definition of "Former Public Servant (FPS)". 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.	Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive? Yes ☐ No ☐	
	If yes, 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; and	
	g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.	

Table 6 - Federal Contractors Program For Employment Equity

In accordance with Articles 5.1.2 under Part 5, please complete the Form below.

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).

Table 7 – Team Certification

Team Certification

Canada believes that there is a strong correlation between the success of an initiative and a Contractor with well-established relationships with its team members e.g. parent organization, affiliated organization, any subsidiary organization and major tier-one subcontractors as applicable.

Therefore, by signing the certification below, the Bidder hereby certifies that:

(i) All of the Bidder's team members identified in its proposal have a signed teaming agreement or signed Contract in respect of the services to be provided under any Contract resulting from this RFP, prior to the bid closing date (A signed letter of intent from a team member is not sufficient);

(ii) Where the team member is a related organization (i.e. parent, affiliated and/or subsidiary organization), the teaming agreement or Contract for the services to which the experience relates must stipulate that the Bidder can rely upon and use the experience of the team member throughout the performance of any resulting Contract; and

(iii) The teaming agreement or Contract must stipulate that the team member whose experience is being presented for evaluation will be actively responsible for the delivery of those services to which the experience relates under any resulting Contract.

If for reasons beyond its control, the Bidder is unable to provide the services of a team member 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. Canada reserves the right to reject any substitute for any reason, at its discretion. 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.

In order to demonstrate that it meets this requirement, the Bidder is requested to provide the following certification:

CERTIFICATION SIGNATURE

We hereby certify compliance with the above noted requirements and have signed teaming agreements that meet the above requirements with the following team members:

(Bidders must enter the names of the organization(s) for which teaming agreements or Contracts are in place).

We also certify that we have the permission from the team members named above to propose their services in relation to the work to be performed. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the team members, of the permission given to the Bidder and of their availability.

We also certify that the signature below is that of a person authorized to sign on behalf of the Bidder.

_____ _____
Signature Date

_____
Name and title of person authorized to sign on behalf of the Bidder

_____
Name of the Bidder

Table 8: RFP Submission Checklist

Supply Chain Security Information (SCSI) (6 hard copies and 1 soft copy on a USB in a format accessible by Canada)	
Form 3 to Part 4 - IT product list and Subcontractor list	☐
Attachment 4 to Part 4: SCSI Network Diagram	☐
Technical Bid (6 hard copy and 1 soft copy on a USB in a format accessible by Canada - can be on the same USB with SCSI)	
Attachment 2 to Part 4 - Evaluation Criteria	☐
Table 1 of Form 1 to Part 4 - RFP Submission Form	☐
Form 2 to Part 4 - Project Reference Check Form	☐
Financial Bid (1 hard copy and 1 soft copy on a separate USB in a format accessible by Canada)	
Annex 3 – Price Schedule	☐
Certifications (1 hard copy and 1 soft copy on a USB - can be on the same USB with the SCSI and Technical Bid)	
Table 2 of Form 1 to Part 4 - Declaration of Convicted Offences	☐
Table 3 of Form 1 to Part 4 - Integrity Provisions	☐
Table 4 of Form 1 to Part 4 - Former Public Servant	☐
Table 5 of Form 1 to part 4 - Work Force Adjustment	☐
Table 6 of Form 1 to Part 4 - Federal Contractors Program For Employment Equity	☐
Table 7 of Form 1 to Part 4 – Team Certification	☐
Security and Financial Requirements	
Annex 2 – Security and Privacy	☐
Annex 4 – Security Requirements Check List (SRCL) and Security Classification Guide (SCG)	☐
Proof of Proposal Test for Top-Ranked Bidder (If requested by Canada)	

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 the projects identified in *Attachment 2 to Part 4 – Technical Evaluation* 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 – Technical Evaluation*)		
(b)	Bidder's Full Legal Name (if the Bidder is a joint venture, the full legal of each member of the joint venture 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/H		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)**