Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.\11, rue Laurier
Gatineau
K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

THERE IS A SECURITY REQUIREMENT ASSOCIATED WITH THIS SOLICITATION

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution

Business Transformation and Systems Integration
Service/Division de transformation des opérations et d'intégrat
Special Procurement Initiative Dir
Dir. des initiatives speciales d'approvisionnement
11 Laurier, Place du Portage III
12C1
Gatineau
Québec

Title - Sujet	
ISS Transformation - RFP	
Solicitation No. - N° de l'invitation	**Date**
EP243-170549/B	2017-03-27
Client Reference No. - N° de référence du client	
20170549	
GETS Reference No. - N° de référence de SEAG	
PW-$$XE-678-31237	
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
678xe.EP243-170549	
Solicitation Closes - L'invitation prend fin	**Time Zone / Fuseau horaire**
at - à 02:00 PM	Eastern Daylight Saving Time EDT
on - le 2017-05-31	
F.O.B. - F.A.B.	
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Oates, Christine	678xe
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(873) 469-3917 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERVICES CANADA
PORTAGE III
11 LAURIER ST
Gatineau
Quebec
K1A0S5
Canada

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
See Herein	

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

Solution Based Informatics Professional Services (SBIPS) Request for Proposal (RFP)

FOR

The Industrial Security Systems Transformation

FOR

Public Works and Government Services Canada

SBIPS REQUEST FOR PROPOSAL (RFP) AND RESULTING CONTRACT CLAUSES

This Request for Proposal (RFP) is issued to solicit bids from pre-qualified suppliers holding a valid Solutions-Based Informatics Professional Services Supply Arrangement (SBIPS SA) issued pursuant to the Request for Supply Arrangement (RFSA) solicitation No. EN537-05IT01.

Unless otherwise specified in this document, all terms and conditions of the SBIPS SA apply and will be incorporated into this SBIPS SA RFP and any resulting contract by reference.

No Contractor is presently performing these services.

Specific terms of this SBIPS SA RFP are as follows:

A. Project Summary

This SBIPS SA RFP is being competed under Tier 2 for Public Works and Government Services Canada.

This SBIPS SA RFP is a requirement involving the following SBIPS Stream(s) of Expertise:

11. Systems Integration

B. Potential Bidders

All Tier 2 SBIPS SA Holders qualified in the above Stream of Expertise are eligible to bid on this requirement.

TABLE OF CONTENTS

LIST OF ANNEXES:

ANNEX A - Statement of Work
- APPENDIX 1 to ANNEX A - Current Business Processes
- APPENDIX 2 to ANNEX A - Key Activities
- APPENDIX 3 to ANNEX A - User Accounts Overview
- APPENDIX 4 to ANNEX A - Legislative, Regulatory and Policy Requirements
- APPENDIX 5 to ANNEX A - Glossary of Terms
- APPENDIX 6 to ANNEX A - Acronyms and Abbreviations

ANNEX B - Price Schedule
ANNEX C - SRCL
ANNEX D - Non-Disclosure Agreement
ANNEX E - Task Authorization Form
ANNEX F - Resource Category Information for Optional Services

LIST OF ATTACHMENTS:

Attachment 1 to Part 4 - Technical Evaluation Criteria

FORMS:

Form 1 to Part 4 - RFP Submission Form
Form 2 to Part 4 - Project Reference Check Form
Form 3 to Part 4 - Bid Solicitation - Financial Bid Form

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 Bidders with instructions on how to prepare their bid;

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

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

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

Part 7 Resulting Contract Clauses: includes 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 This bid solicitation is being issued to satisfy the requirement of the Industrial Security Sector (ISS) of Public Works and Government Services Canada, (the "**Client(s)**") for Solutions-based Informatics Professional Services (SBIPS) under the SBIPS Supply Arrangement (SA) method of supply.

1.2.2 It is intended that this solicitation will result in the award of one (1) Contract, for twenty-nine (29) months, plus four (4) irrevocable options allowing Canada to extend the term of the Contract, each for a period of six (6) months.

1.3 Debriefings

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

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

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

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.

The 2003 Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

"Subsection 3 of Section 01, Integrity Provisions - Bid of Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:

3. List of Names

    a. Bidders who are incorporated or who are a sole proprietorship, including those bidding as a joint venture, have already provided a list of names of all individuals who are directors of the Bidder, or the name of the owner(s), at the time of submitting an arrangement under the Request for Supply Arrangement (RFSA).

    b. These Bidders must immediately inform Canada in writing of any changes affecting the list of directors during this procurement process.

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

Delete: 60 days
Insert: 365 days

2.1.1 *SACC* Manual Clauses

A7035T (2007-05-25), List of Proposed Subcontractors

2.2 Submission of Bids

Bids must be submitted only to PWGSC Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation. Bids transmitted to PWGSC by electronic mail will not be accepted.

Due to the nature of the bid solicitation, bids transmitted by facsimile 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 ten (10) calendar days before the bid closing date. Enquiries received after that time may not be answered.

The Contracting Authority for the solicitation is:

Christine Oates
Contracting Authority
Acquisitions Program
PWGSC

Email: Christine.Oates@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 reasons for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular Bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled “Enquiries - Bid Solicitation”. Canada will have the right to accept or reject any or all suggestions.

2.6 Bidders’ Conference

A bidders' conference will be held at 2745 Iris Street, Ottawa, Ontario on 5 May 2017. The conference will begin at 09:30 EDT, in the First Floor Boardroom. 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 28 April 2017.

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.

2.7 Volumetric Data

If volumetric data is provided to Bidders in this solicitation document, which could contain current and historical data, the inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada’s future volumetric data 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 and Canada will not be liable for any business loss the winning Bidder may claim during the performance of the contract, in the event that the actual volumetric data deviates from the one provided in this RFP.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

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

(a) Section I: Technical Bid
- 7 hard copies; and
- 2 soft copies on USB in a format compatible with Microsoft Office Suite 2010 or Adobe Acrobat XI;

(b) Section II: Financial Bid
- 1 hard copy; and
- 2 soft copies on a separate USB in a format compatible with Microsoft Office Suite 2010 or Adobe Acrobat XI; and

(c) Section III: Certifications
- 2 hard copies; and
- 2 soft copies on USB in a format compatible with Microsoft Office Suite 2010 or Adobe Acrobat XI (Section III: Certifications should be on the same medium as Section I: Technical Bid);

(d) 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.

(e) Prices should appear in the financial bid only. Prices should not be indicated in any other section of the bid.

3.1.2 Format of Bid: Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

(a) Use 8.5 x 11 inch (216 mm x 279 mm) paper;

(b) Use a numbering system that corresponds to the bid solicitation;

(c) Include a title page: The first page of each volume of the bid, after the cover page, should be the Title Page, which should contain:

(i) The title of the bid and the section number;
(ii) The name and address of the Bidder;
(iii) The name, address and telephone number of the Bidder's representative;
(iv) The bid date; and,
(v) The bid solicitation number.

(d) Include a table of contents: The page following the Title 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 sub-sections with associated page numbers. It should also list the associated tables, figures, and annexes or appendices contained in the part of the bid to which it refers.

(e) Include headers and footers: Each subsequent page of each volume of the bid should include a header and/or footer that include the following information:

(i) The title of the bid;
(ii) The name of the Bidder;
(iii) The bid date; and,
(iv) The page number.

(f) Use of Cross References: Where the Bidder uses cross references to Information contained in the bid, the reference should include the following details:

(i) The technical bid part number;
(ii) The document name;
(iii) The document section name and number (if applicable); and,
(iv) The page number.

3.1.3 Canada's Policy on Green Procurement: 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.

To assist Canada in reaching its objectives, Bidders should:

(a) Use paper containing fiber 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 color printing, printing double sided/duplex, using staples or clips instead of cerlox, duo tangs or binders.

3.1.4 No Conditional Bids

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

3.1.5 Submission of Only One Bid

A Bidder will be permitted to submit only one bid in response to this bid solicitation. If a Bidder participates in more than one bid (participating means being part of the Bidder, not being a subcontractor), Canada will provide the Bidder with 2 working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified. 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.

3.1.6 Bidder's Additional Instructions

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.

3.2 Section I: Technical Bid

3.2.1 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.

3.2.2 It is requested that the Technical Bid include submission of the Bidder's response to Attachment 1 to Part 4 – Technical Evaluation, Form 1 to Part 4 – RFP Submission Form, Form 2 to Part 4 – Project Reference Check Form, 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.

3.2.3 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.

3.2.4 Part 4, Evaluation Procedures and Basis of Selection contains additional instructions that Bidders should consider when preparing their technical bid.

3.3 Section II: Financial Bid

3.3.1 The Bidder must provide its Financial Bid in accordance with ANNEX B - Price Schedule and Form 3 to Part 4 – Bid Solicitation – Financial Bid Form.

3.3.2 Exchange Rate Fluctuation

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

C3011T (2013-11-06), Exchange Rate Fluctuation

3.4 Section III: Certifications and Additional Information

Bidders must submit the certifications and additional information required under Part 5.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

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 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 may result in the bid being declared non-responsive. If additional time is required by the Bidder, Canada may grant an extension at its sole discretion.

4.1.5 Nothing in the bid evaluation process will 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.

4.1.6 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 Technical Evaluation

4.2.1 **Mandatory Technical Criteria:** Each bid will be evaluated for compliance with the mandatory requirements of the bid solicitation. All elements of the bid solicitation that are mandatory requirements are identified specifically with the words "must" or "mandatory". Bids that do not comply with each and every mandatory requirement will be considered non-responsive and be disqualified. Mandatory evaluation criteria and/or evaluation processes are described under Attachment 1 to Part 4 Technical Evaluation.

4.2.2 **Point-Rated Technical Criteria:** Where Point-Rated Technical Criteria are specified in the RFP, each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly. Point-rated evaluation criteria and/or evaluation processes are described under Attachment 1 to Part 4 Technical Evaluation.

4.2.3 **Technically Responsive Bid:** A technically responsive bid is a bid that meets all of the mandatory requirements and obtains the required minimum points specified in the bid solicitation for the criteria that are subject to point rating.

4.2.4 Reference Checks

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

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

4.2.4.3 For the purpose of this evaluation, reference checks may be used to verify and validate the Bidder's bid response. If a reference check is performed, Canada will conduct the reference check in writing by e-mail. Canada will send the reference check request directly to the client contact for the project reference provided by the Bidder. The client contact will have 5 working days (or a longer period otherwise specified in writing by the Contracting Authority) from the date that Canada's e-mail was sent, to respond to Canada.

4.2.4.4 The client contact will be required, within 2 working days after Canada sends out the reference check request, to acknowledge the receipt of the reference check request and identify his or her willingness and availability to conduct such a reference check. If Canada has not received the required response from the client contact, Canada will notify the Bidder by e-mail, to allow the Bidder to contact its client contact directly to ensure that he or she responds to Canada within the allotted time.

4.2.4.5 Notwithstanding section 4.2.4.4, if the client contact is unavailable when required during the evaluation period, the Bidder will be requested to provide an alternate client contact for the same referenced project. Bidders will only be provided with this opportunity once for each referenced project and only if the original client contact is unavailable to respond. The process as described in 4.2.4.4 is applicable for the reference check with the alternate client contact. The period to respond for either the original client contact, or the alternate client contact, will be a total of 5 working days (or a longer period otherwise specified in writing by the Contracting Authority) in accordance with 4.2.4.4.

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

4.2.4.7 Non-consideration of the Bidder's claimed project experience will result if:

(a) the reference check client contact fails to timely respond to Canada's request;

(b) the reference check client contact states he or she is unable or unwilling to provide the information requested;

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

(d) the reference check client contact organization and/or client contact was affiliated with the Bidder during the referenced project; if the client contact organization and/or contact has ever been or is currently affiliated with the Bidder; or if the client contact organization is an entity that does not deal at arm's length with the Bidder.

4.2.4.8 Where non-consideration of a Bidder's claimed project experience, as a result of 4.2.4.7, for any Mandatory Requirements in the Technical Evaluation (Attachment 1 to Part 4) results in the Bidder

not meeting one or more mandatory requirements, the bid will be declared non-responsive in accordance with section 4.5 Basis of Selection.

4.2.4.9 Non-consideration of a Bidder's claimed project experience, as a result of 4.2.4.7, for the Rated Requirements in the Technical Evaluation (Attachment 1 to Part 4) will result in the Bidder not being awarded the points associated with the respective rated criterion. If this results in the Bidder not achieving the pass mark of point-rated evaluation, the bid will be declared non-responsive in accordance with section 4.5 Basis of Selection.

4.3 Financial Evaluation

4.3.1 Unless otherwise specified in the RFP, the financial evaluation will be conducted by calculating the Total Evaluated Bid Price as indicated in section 4 of Form 3 to Part 4 – Bid Solicitation – Financial Bid Form. The Bidder must provide firm, all inclusive, rates for the firm price Work and if applicable, firm, all inclusive per diem rates for resource categories in accordance with the bid solicitation, which may include an initial contract period and option periods.

4.3.2 The financial evaluation will also be conducted in accordance with the following SACC Manual Clause:

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

4.3.3 Substantiation of Professional Services Rates

4.3.3.1 In Canada's experience, Bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates for professional services bid, Canada may require price support for any rates proposed (either for all or for a specific Resource Category). If Canada requests price support, it will be requested from all responsive Bidders proposing a rate that is at least 20% lower than the median rate bid by all responsive Bidders for the relevant Resource Category or Categories. Where Canada requests price support, the following information is required:

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

(b) in relation to the invoice in (a), evidence from the Bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work for the category of resource being assessed for an unreasonably low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation;

(c) with respect to each contract for which an invoice is submitted as substantiation, a résumé for the resource that provided the services under that contract that demonstrates that, in relation to the resource category for which the rates are being substantiated, the resource would meet the mandatory requirements and achieve any required pass mark for any rated criteria; and

(d) the name, telephone number and, if available, e-mail address of a contact person at the customer who received each invoice submitted under (a), so that Canada may verify any information provided by the Bidder.

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

4.4 Basis of Selection

4.4.1 Basis of Selection – Highest Combined Rating of Technical Merit (70%) and Price (30%)

4.4.1.1 To be declared responsive, a bid must:

(a) comply with all the requirements of the bid solicitation; and

(b) meet all mandatory criteria; and

(c) obtain the required minimum of 1750 points overall for the technical evaluation criteria which are subject to point rating. The rating is performed on a scale of 2500 points.

4.4.1.2 The responsive bid that obtains the highest Total Bidder Score will be recommended for award of a contract. The Total Bidder Score is calculated as follows:

Total Bidder Score = Total Technical Score + Total Financial Score

4.4.1.3 In the event of identical Total Bidder Scores occurring, the Bidder whose bid achieves the highest Total Technical Score will become the top-ranked Bidder.

4.4.1.4 If more than one Bidder is ranked first because of identical Total Bidder Scores and identical Total Technical Scores, the Bidder obtaining the highest score for the first Point Rated Evaluation Criteria, in order of appearance in Attachment 1 to Part 4, will become the top-ranked Bidder and recommended for award of the contract.

4.4.1.5 When necessary, this process will continue through each point rated criteria, in order of appearance in Attachment 1 to Part 4, until all the point rated scores have been used.

4.4.1.6 If two or more Bidders are still tied after 4.4.1.3, 4.4.1.4 and 4.4.1.5 above, a “coin flip” method will be used to determine the top-ranked Bidder.

4.4.1.7 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.

4.4.1.8 Notification of Evaluation Result

All SA Holders who respond to a SBIPS RFP will be notified in writing regarding the outcome of the RFP process. This notice will include the following information:

(a) Solicitation Number;
(b) Company name of winning Bidder including total points scored;
(c) Total value of Contract awarded;
(d) Number of responses received by the Contracting Authority; and
(e) Total points scored of the Bidder (Note: Bidders will only receive their own total points scored and not the score of the other Bidders)

4.4.1.9 Example

The following Table illustrates an example where the selection of the bid is determined by 70/30 ratio of the technical and pricing score, respectively. The maximum rated points in this example is 100. The lowest priced technically compliant proposal is allocated the maximum points of 30 and other price proposals are pro-rated accordingly.

Example of Bid Selection			
Highest Combined Rating of Technical Merit (70%) and Price (30%)			
Bidder	**Bidder 1**	**Bidder 2**	**Bidder 3**
Rated Points Obtained	83	79	75
Total Evaluated Bid Price	$60,000	$55,000	$50,000
Calculation	**Total Technical Score**	**Total Financial Score**	**Total Bidder Score**
Bidder 1	83/100x70 = 58.10	50/60x30 = 25.00	**83.10**
Bidder 2	79/100x70 = 55.30	50/55x30 = 27.27	**82.57**
Bidder 3	75/100x70 = 52.50	50/50x30 = 30	**82.50**
Winning Bidder	**Bidder 1**		

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

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 Contract period.

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

5.1 Certifications Precedent to Contract Award and Additional Information

The Bidder is requested to complete and submit Form 1 to Part 4 – RFP Submission Form with the bid. 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 Former Public Servant Certification

(a) 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 the information required below before Contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

(b) **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:

(i) an individual;

(ii) an individual who has incorporated;

(iii) a partnership made of former public servants; or

(iv) 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-8.

(c) **Former Public Servant in Receipt of a Pension**

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

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

(i) name of former public servant;

(ii) date of termination of employment or retirement from the Public Service.

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

(d) **Work Force Adjustment Directive**

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

If so, the Bidder must provide the following information:

(i) name of former public servant;

(ii) conditions of the lump sum payment incentive;

(iii) date of termination of employment;

(iv) amount of lump sum payment;

(v) rate of pay on which lump sum payment is based;

(vi) period of lump sum payment including start date, end date and number of weeks;

(vii) number and amount (professional fees) of other Contracts subject to the restrictions of a work force adjustment program.

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

5.1.2 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 period of the Contract.

The Bidder must provide the Contracting Authority with a completed Form 1 to Part 4 – RFP Submission Form, including the Federal Contractors Program certification, before contract award.

If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed Form 1 to Part 4 – RFP Submission Form for each Joint Venture.

5.1.3 Team Certification

The Bidder must certify that it meets the following mandatory requirements otherwise its bid will be declared non-responsive:

a. The Bidder must identify and provide all its Team Members in the bid and have signed formal Teaming Agreement(s) or signed Contract(s) 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);

b. The Bidder must obtain the permission from the Team Members to use their service experience in response to the RFP requirements;

c. Where the Team Member is a related organization (i.e. parent, affiliated and/or subsidiary organization), the Teaming Agreement(s) or Contract(s) 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;

d. 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, and

e. 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.

If the Bidder is awarded a Contract, and for reasons beyond its control, the Team Member of the Bidder is unable to provide the services to which the experience relates and which was used to meet evaluation criteria of the RFP, the Bidder may propose a substitute with equivalent or better qualifications and experience. The Bidder must advise the Contracting Authority within 15 business days 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. If the Bidder cannot provide a satisfactory substitute for the original proposed Team Member, Canada may terminate the Contract for default.

For greater clarity, the following situations may be considered as beyond the control of the Bidder: death, sickness, retirement, resignation, dismissal for cause or termination of an agreement for default of critical corporate resources that would prevent the Team Member from delivering services under the Contract; or where the Team Member is bankrupt or, for whatever reason, its activities are rendered inoperable for an extended period; or a merger or acquisition of the Team Member.

PART 6 – SECURITY AND OTHER REQUIREMENTS

6.1 Security Requirements

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

(a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

(b) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;

(c) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

(d) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

6.1.2 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.

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

(a) _____ (the Contractor) agrees to supply to the Client the goods and services described in the Contract, including all the ANNEXES, in accordance with and at the prices set out in the Contract.

(b) **Client:** Under the Contract, the "**Client**" is Public Works and Government Services Canada (PWGSC) or interchangeably Public Services and Procurement Canada (PSPC).

(c) **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 Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

(d) **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.

(e) **Option to Add New Consultant Categories:** The Contractor grants Canada the right to add new Resource Categories for the provision of services that are part of the work-scope of the Contract as described in the Statement of Work at ANNEX A, as needed and at any time during the Contract, or during option periods, if exercised, under the same conditions and at prices which are to be negotiated in accordance with the ANNEX B – Price Schedule. Adding new Resource Categories will require a contract amendment issued by the Contracting Authority.

7.2 Task Authorization

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

7.2.1 Task Authorization Process

7.2.1.1 Work described at Section 8 of ANNEX A - Statement of Work, will be performed under the Contract on an “as and when required basis”.

7.2.1.2 With respect to the Work mentioned under paragraph 7.2.1.1 of this clause,

i. 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;

ii. the TA Authority and limit will be determined in accordance with paragraph 7.2.1.3 of this clause;

iii. 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; and

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

7.2.1.3 **TA Authority and Limit**

i. 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.
ii. The authority specified under paragraph i. of this clause is granted subject to the sum specified in the Contract in subsection 7.8.2 Limitation of Expenditure not being exceeded.

7.2.1.4 **TA Request**

For each task or revision of a previously authorized task, the Project Authority will provide the Contractor with the Task Authorization Form (ANNEX E) including a description of the task and minimum mandatory requirements using ANNEX F – Resource Category Information for Task Authorizations, and within the scope of ANNEX A – Statement of Work, containing as a minimum:

i. the task or revised task description of the Work requested, including:
   (a) the details of the activities or revised activities to be performed;
   (b) a description of the deliverables or revised deliverables to be submitted;
   (c) the language profile of the resources required; and
   (d) a schedule or revised schedule indicating completion dates for the major activities or submission dates for the deliverables, or both, as applicable;
ii. the Contract security requirements applicable to the task or revised task;
iii. the Contract basis (bases) of payment applicable to the task or revised task*;* and
iv. the Contract method(s) of payment applicable to the task or revised task and, as applicable, the associated schedule of milestones.

7.2.1.5 **TA Response**

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:

i. the total estimated cost proposed for performing the task or, as applicable, revised task;
ii. a breakdown of that cost in accordance with ANNEX B – Price Schedule, to be provided, as applicable, per milestone contained in the Schedule of Milestones; and
iii. for each resource proposed by the Contractor for the performance of the Work requested:
   (a) the name of the proposed resource;
   (b) the resume of the proposed resource; and
   (c) a demonstration that the proposed resource meets:
      (i) the Contract security requirements;
      (ii) the requested experience and minimum mandatory qualifications identified in the TA and in ANNEX F – Resource Category Information for Task Authorizations; and
      (iii) Whether the TA request is solution based or resource based, the Contractor must substantiate its TA response by identifying the proposed resource categories and demonstrated experience in accordance with ANNEX F – Resource Category

Information for Task Authorizations, as well as price substantiation in accordance with ANNEX B – Price Schedule.

The above applies only to TAs where Canada will pay for Work that is not otherwise covered by fixed fees in the Contract.

7.2.1.6 **TA Approval and Issuance**

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

(a) the request submitted to the Contractor pursuant to paragraph 7.2.1.4 of this clause;
(b) the Contractor's response received, submitted pursuant to paragraph 7.2.1.5 of this clause; and
(c) the agreed total estimated cost for performing the task or, as applicable, revised task; and, as applicable, the breakdown of that cost per milestone.

ii. 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 7.2.1.5 of this clause.

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

7.2.1.7 **Periodic Usage Reports - Contracts with TAs**

i. 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.

ii. 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 iii. and iv. 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.

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

(a) the TA number appearing on the TA form;
(b) the date the task was authorized appearing on the TA form;
(c) the total estimated cost of the task (Applicable Taxes extra) before any revisions appearing on the TA form; and
(d) the following information appearing on the TA form must be included for each authorized revision, starting with revision 1, then 2, etc.:
    (i) the TA revision number;
    (ii) the date the revision to the task was authorized;
    (iii) the authorized increase or decrease (Applicable Taxes extra);
    (iv) the total estimated cost of the task (Applicable Taxes extra) after authorization of the revision;
    (v) the total cost incurred for the task (as last revised, as applicable), Applicable Taxes extra;

(vi) the total cost incurred and invoiced for the task (as last revised, as applicable), Applicable Taxes extra;
(vii) the total amount of Applicable Taxes invoiced;
(viii) the total amount paid, Applicable Taxes included;
(ix) the start and completion date of the task (as last revised, as applicable); and
(x) the active status (i.e., the percentage of the work completed) of the task (as last revised, as applicable) with an explanation (as applicable).

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

(a) the total cost incurred for all authorized tasks inclusive of any revisions, Applicable Taxes extra;
(b) the total cost incurred and invoiced for all authorized tasks inclusive of any revisions, Applicable Taxes extra;
(c) the total amount of Applicable Taxes invoiced for all authorized tasks inclusive of any revisions; and
(d) the total amount paid for all authorized tasks inclusive of any revisions, Applicable Taxes extra.

7.2.1.8 **Consolidation of Task Authorizations for Administrative Purposes**

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

7.2.1.9 **Canada's Obligation**

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.

7.3 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.

7.3.1 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) Supplemental General Conditions:

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

i. 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services; and

ii. 4007 (2010-08-16), Supplemental General Conditions - Canada to Own Intellectual Property Rights in Foreground Information.

7.4 Security Requirement

7.4.1 The Contractor must, at all times during the performance of the Contract/Standing Offer, hold a valid **Facility Security Clearance (FSC) at the level of SECRET,** issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

7.4.2 The Contractor personnel requiring access to **NON RESTRICTED PROTECTED** information, assets or sensitive work site(s) must **EACH** hold a valid **RELIABILITY STATUS or SECRET, as required,** granted or approved by CISD/PWGSC.

7.4.3 The Contractor personnel requiring access to **RESTRICTED PROTECTED** information, assets or sensitive work site(s) **must be a permanent resident of Canada or a citizen of Canada and**

must EACH hold a valid **RELIABILITY STATUS or SECRET, as required,** granted or approved by CISD/PWGSC.

7.4.4 The Contractor personnel requiring access to **NATO UNCLASSIFIED** information or assets do not require to hold a personnel security clearance; however, the Contractor must ensure that the NATO Unclassified information is not releasable to third parties and that the "need to know" principle is applied to personnel accessing this information.

7.4.5 The Contractor personnel requiring access to **NATO RESTRICTED** information or assets **must be citizens of a NATO member country or a permanent resident of Canada** and **EACH** hold a valid **RELIABILITY STATUS** or its equivalent, granted or approved by the appropriate delegated NATO Security Authority.

7.4.6 The Contractor **MUST NOT** remove any **PROTECTED** information from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restriction.

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

7.4.8 The Contractor must comply with the provisions of the:
(a) Security Requirements Check List and security classification guide, attached at ANNEX C;
(b) Industrial Security Manual (Latest Edition).

7.4.9 **Personal Information**

(a) The Contractor acknowledges that Canada is bound by the *Privacy Act*, R.S., 1985, c. P-21, with respect to the protection of personal information as defined in the Act. The Contractor must keep private and confidential any such personal information collected, created or handled by the Contractor under the Contract, and must not use, copy, disclose, dispose of or destroy such personal information except in accordance with this clause and the delivery provisions of the Contract.

(b) All such personal information is the property of Canada, and the Contractor has no right in or to that information. The Contractor must deliver to Canada all such personal information in whatever form, including all working papers, notes, memoranda, reports, data in machine-readable format or otherwise, and documentation which have been made or obtained in relation to the Contract, upon the completion or termination of the Contract, or at such earlier time as Canada may request. Upon delivery of the personal information to Canada, the Contractor will have no right to retain that information in any form and must ensure that no record of the personal information remains in the Contractor's possession.

(c) 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.

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

(i) Applicant identification information (e.g. names, addresses, company profiles, résumés, work experience, previous Contracts completed, and users).
(ii) Applicant financial data (e.g. credit information).
(iii) Procedures, forms, computer systems and data file layouts, and Internet Web sites, etc.

(iv) Contact information (including business name), biographical information, educational information, financial information, evaluations/assessments, other identification number (e.g. Business Number) and signature.

7.4.10 **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 ISS 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 Project Authority;

(iv) Protect sensitive information and safeguard against theft, including identity theft or unauthorized third parties acting on behalf of the Project Authority, 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 ISS Disposition Authority.

7.4.10 **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.

7.5 Contract Period

(a) **Contract Period**: The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

i. The "**Initial Contract Period**", which begins on the date the Contract is awarded and ends 29 months later; and

ii. The period during which the Contract is extended, if Canada chooses to exercise any options set out in the Contract.

(b) **Option to Extend the Contract:**

i. The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to four (4) additional six (6) month period(s) under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

ii. Canada may exercise this option at any time by sending a written notice to the Contractor at least thirty (30) calendar days 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 formal Contract amendment.

7.6 Authorities

(a) **Contracting Authority (To be completed at time of Contract award)**

The Contracting Authority for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
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.

(b) **Technical Authority (To be completed at time of Contract award)**

The Technical Authority for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
E-mail address: _____

The Technical Authority 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 Technical Authority; however, the Technical 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.

(c) **Contractor's Representative (To be completed at time of Contract award)**

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
E-mail address: _____

7.7 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 web sites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.8 Payment

7.8.1 Basis of Payment

For all Basis of Payment outlined below Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been authorized, in writing, by the Contracting Authority before their incorporation into the Work.

(a) **Firm Lot Price**

For the Work described in Sections 1 through 8 of ANNEX A - Statement of Work, in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid in accordance with ANNEX B – Price Schedule.

(b) **Professional Services Provided under a Task Authorization with a Maximum Price**

For professional services requested by Canada, in accordance with an approved Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked under each Task Authorization and any resulting deliverables in accordance with the firm all-inclusive per diem rates set out in ANNEX B – Price Schedule of this contract, Applicable Taxes extra. Partial days and extra hours will be prorated based on actual hours worked based on a 7.5-hour workday.

(c) **Firm Lot Price TA**

When the applicable Basis of Payment specified in a TA authorized and issued under the Contract is firm lot price, in consideration of the Contractor satisfactorily completing all of its obligations under the authorized TA, the Contractor will be paid the firm lot price stipulated in the authorized TA, as determined in accordance with the Price Schedule cost elements in ANNEX B. Customs duties are included and Applicable Taxes are extra.

(d) **Milestone Payments**

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the TA and Contract and the payment provisions of the TA and Contract in accordance with a duly completed and authorized Claim for Progress Payment using PWGSC-TPSGC 1111.

(e) **Progress Payments**

Canada will make progress payments in accordance with the TA and Contract and the payment provisions of the TA and Contract in accordance with a duly completed and authorized Claim for Progress Payment using PWGSC-TPSGC 1111.

(f) **Professional Services Not Provided under a Task Authorization**

For the provision of professional services, the Contractor will be paid for actual time worked, in accordance with the firm all-inclusive per diem rates set out in ANNEX B - Price Schedule, Applicable Taxes extra. Partial days and extra hours will be prorated based on actual hours worked based on a 7.5-hour workday.

(g) **GST/HST**: Estimated Cost: *(to be confirmed at contract award)*

(h) **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. The Contractor will be able to charge for time spent travelling from the National Capital Region to Canada's work site(s), if such travel is requested by the Project Authority, 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.

(i) **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.

7.8.2 Limitation of Expenditure

(a) The Contractor will be reimbursed for the costs reasonably and properly incurred in the performance of the Work, as determined in accordance with the Price Schedule in ANNEX B, to a limitation of expenditure not to exceed $ _____*(to be confirmed at contract award)*. Customs duties are included and 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:

i. when it is 75 percent committed;
ii. four (4) months before the contract expiry date; or
iii. 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.

7.8.2.1 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.

7.8.3 Method of Payment

(a) **Firm Lot Price**

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

i. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
ii. all such documents have been verified and accepted by Canada; and
iii. the Work delivered has been accepted by Canada.

(b) **Task Authorizations with a Maximum Price**

For each individual Task Authorization issued under the Contract that contains a maximum price:

i. 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 under each Task Authorization to support the charges claimed in the invoice.

ii. Once Canada has paid the maximum price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the Task Authorization, all of which is required to be performed for the maximum price. If the work described in the

Task Authorization is completed in less time than anticipated, and the actual time worked (as supported by the time sheets) at the rates set out in the Contract is less than the maximum price, Canada is only required to pay for the time spent performing the work related to that Task Authorization.

(c) **Task Authorizations with a Firm Price - Lump Sum Payment on Completion**

Canada will pay the Contractor upon completion and delivery of all the Work associated with the Task Authorization in accordance with the payment provisions of the Contract if:

i. an accurate and complete invoice for work under each Task Authorization, and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii. all such documents have been verified and accepted by Canada; and

iii. the Work delivered has been accepted by Canada.

(d) **Milestone Payments**

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

i. an accurate and complete claim for payment using PWGSC-TPSGC 1111, Claim for Progress Payment, and any other document required by the Contract have been submitted for each portion of work (TA/Contract) and accepted by Canada in accordance with the invoicing; instructions provided in the Contract;

ii. all the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives; and

iii. all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

(e) **Progress Payments**

Canada will make progress payments in accordance with the payment provisions of the TA and Contract, no more than once a month, for cost incurred in the performance of the Work, up to 90 percent of the amount claimed and approved by Canada if:

i. an accurate and complete claim for payment using form PWGSC-TPSGC 1111 Claim for Progress Payment for each portion of work (TA/Contract), and any other document required by the TA and Contract have been submitted and accepted by Canada in accordance with the invoicing instructions provided in the Contract;

ii. the amount claimed is in accordance with the Basis of Payment and TA;

iii. the total amount for all progress payments paid by Canada does not exceed 90 percent of the total amount to be paid under the TA; and

iv. all certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives.

The balance of the amount payable will be paid in accordance with the payment provisions of the TA and Contract upon completion and delivery of all work required under the TA if the Work has been accepted by Canada and a final claim for the payment is submitted.

Progress payments are interim payments only. Canada may conduct a government audit and interim time and cost verifications and reserves the rights to make adjustments to the Contract from time to time during the performance of the Work. Any overpayment resulting from progress payments or otherwise must be refunded promptly to Canada.

(f) **Monthly Payment:**

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

i. an accurate and complete invoice for each portion of work and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii. all such documents have been verified and accepted by Canada; and

iii. the Work performed has been accepted by Canada.

7.8.4 Time Verification

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contract must repay any overpayment with 30 calendar days, at Canada's request.

7.8.5 Payment Credits

(a) **Failure to Provide Resource**

i. If the Contractor does not provide a required professional services resource that has all the required qualifications within the time prescribed by the Contract, the Contractor must credit to Canada an amount equal to the per diem rate (based on a 7.5-hour workday) of the required resource for each day (or partial day) of delay in providing the resource, up to a maximum of 10 days.

ii. **Corrective Measures**: If credits are payable under this Article for two consecutive months or for three months in any 12-month period, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Client and the Contracting Authority and 20 working days to rectify the underlying problem.

iii. **Termination for Failure to Meet Availability Level**: In addition to any other rights it has under the Contract, Canada may terminate the Contract for default in accordance with the General Conditions by giving the Contractor three months' written notice of its intent, if any of the following apply:

(1) the total amount of credits for a given monthly billing cycle reach a level of 10% of the total billing for that month; or

(2) the corrective measures required of the Contractor described above are not met.

This termination will be effective when the three month notice period expires, unless Canada determines that the Contractor has implemented the corrective measures to Canada's satisfaction during those three months.

(b) **Period during Which Credits Apply**: the credits apply throughout the Contract Period.

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

(d) **Canada's Right to Obtain Payment**: The 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.

(e) **Canada's Rights and Remedies Not Limited**: Nothing in this Article 7.8.5 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.

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

7.8.6 No Responsibility to Pay for Work Not Performed due to Closure of Government Offices

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.

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.

7.8.7 SACC Manual Clauses – Payment

The following SACC manual clauses apply to and form part of this Contract:

(a) A9117C (2007-11-30), T1204 - Direct Request by Customer Department;

(b) C6001C (2013-04-25), Limitation of Expenditure;

(c) C0305C (2014-06-26), Cost Submission - Limitation of Expenditure or Ceiling Price;

(d) C0705C (2010-01-11), Discretionary Audit; and

(e) C2000C (2007-11-30), Taxes - Foreign-based Contractor [**Note to Bidders:** if applicable, otherwise this clause will be deleted]

7.9 Invoicing Instructions

7.9.1 Invoicing Instructions - General

(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 B – 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 B of the Contract, including any charges for work performed by subcontractors.

(d) The Contractor must provide the original of each invoice or Claim for Progress Payment to the Project Authority and upon request, the Contractor must provide a copy of any invoices or Claim for Progress Payment to 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.

7.9.2 Invoicing Instructions – Progress Payment Claim – Supporting Documentation required

(a) The Contractor must submit a claim for payment using form PWGSC-TPSGC 1111, Claim for Progress Payment.

Each claim must show:

i. all information required on form PWGSC-TPSGC 1111;

ii. all applicable information detailed under the section entitled "Invoice Submission" of the general conditions;

iii. a list of all expenses (if applicable); and

iv. the description and value of the milestone claimed as detailed in the Contract.

(b) Each claim must be supported by:

i. a copy of the invoices, receipts, vouchers for all direct expenses, travel and living expenses; and

ii. a copy of the monthly progress report.

(c) The Contractor must prepare and certify one original and two (2) copies of the claim on form PWGSC-TPSGC 1111, and forward it to the Project Authority identified under the section entitled "Authorities" of the Contract for appropriate certification after inspection and acceptance of the Work takes place, and onward submission to the Payment Office for the remaining certification and payment action.

(d) The Contractor must not submit claims until all work identified in the claim is completed.

7.10 Certifications and Additional Information

7.10.1 Compliance

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.

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

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html). The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.11 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in *(to be confirmed at contract award)* at, Canada.

7.12 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) these Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;

(b) the Supplemental General Conditions, in the following order:

i. 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services;

ii. 4007 (2010-08-16), Supplemental General Conditions - Canada to Own Intellectual Property Rights in Foreground Information.

(c) General Conditions 2035 (2016-04-04);

(d) ANNEX A - Statement of Work;

(e) ANNEX B - Price Schedule;

(f) ANNEX C - Security Requirements Check List;

(g) ANNEX D - Non-Disclosure Agreement;

(h) ANNEX E – Task Authorization Form

(i) ANNEX F – Resource Category Information for Task Authorization

(j) Supply Arrangement EN537-05IT01/*XXX*/EI;

(k) the signed Task Authorizations (including all of its annexes, if any); and

(l) the Contractor's bid dated _____ (insert date of bid), as amended _____ (insert date(s) of amendment(s) if applicable), 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 a web link) in the bid.

[**Note to Bidders:** The Contractor's bid date will be completed with the information provided in its bid.]

7.13 Foreign Nationals

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

[**Note to Bidders:** Either this clause or the one that follows, whichever applies (based on whether the successful Bidder is a Canadian Contractor or Foreign Contractor), will be included in any resulting Contract.]

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

7.14 Insurance Requirements

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

7.15 Limitation of Liability

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

7.15.2 First Party Liability:

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

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

ii. physical injury, including death.

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

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

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

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

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

ii. any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of 0.75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1,000,000.00.

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 $1,000,000.00, 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.

7.15.3 Third Party Claims:

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

(b) If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount

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

(c) The Parties are only liable to one another for damages to third parties to the extent described in this paragraph 7.15.3.

7.16 Joint Venture Contractor

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

(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 the 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 solidarity 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 provisions of the General Conditions.

(f) The Contractor acknowledges that all security requirements in the Contract apply to each member of the joint venture Contractor.

7.17 Professional Services - General

(a) The Contractor must provide professional services on request as specified in this Contract. All resources provided by the Contractor must meet the qualifications described in the Task Authorization Form (including those relating to previous experience, professional designation, education, and language proficiency and security clearance) and must be competent to provide the required services by any delivery dates described in the Contract.

(b) If the Contractor fails to deliver any deliverable (excluding delivery of a specific individual) or complete any task described in the Contract on time, in addition to any other rights or remedies available to Canada under the Contract or the law, Canada may notify the Contractor of the deficiency, in which case the Contractor must submit a written plan to the Technical Authority within 10 working days detailing the actions that the Contractor will undertake to remedy the deficiency. The Contractor must prepare and implement the plan at its own expense.

7.18 Replacement of Team Members

(a) If for reasons beyond its control, the Team Member of the Contractor is unable to provide the services to which the experience relates and which was used to meet evaluation criteria of the RFP, the Contractor may propose a replacement with equivalent or better qualifications and experience. The Contractor must advise the Contracting Authority within 15 business days of the reason for the replacement and provide the name, qualifications and experience of the proposed replacement. Canada reserves the right to reject any replacement for any reason, should Canada consider the replacement's qualifications and experience to be lesser than its predecessor. If the Contractor cannot provide a satisfactory replacement for the originally proposed Team Member, Canada may terminate the Contract for default. For clarity the following situations may be considered as beyond the control of the Contractor: the Team Member terminates their arrangement with the Contractor; or the Contractor terminates their arrangement with the Team Member for cause; or the Team Member is bankrupt or where, for whatever reason, its activities are rendered inoperable for an extended period; or a merger or acquisition of the Team Member.

(b) Where Canada becomes aware that a Team Member identified under the Contract to provide services has not been provided or is not performing, the Contracting Authority may elect to:

i. 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 assess the information provided under(a) above or, if it has not yet been provided, require the Contractor to propose a replacement to be evaluated by Canada. The replacement must have similar qualifications and experience that meet or exceed those obtained for the original Team Member and be acceptable to Canada;

ii. Upon assessment of the proposed replacement, Canada may accept the replacement, exercise the rights in (b) i. above, or require another replacement.

(c) The Contractor must not, in any event, allow performance of the Work by unauthorized replacement Team Members. The Contracting Authority may order that a Team Member 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 a Team Member to stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.

(d) The obligations in this section apply despite any changes that Canada may have made to the Client's operating environment.

7.19 Timely Problem Identification

(a) The Contractor must immediately advise the Contracting and Technical Authorities in writing of any and all situations or difficulties that the Contractor considers will have a significant impact upon the scope of the Work, expected deliverables, delivery schedule, person-power or cost to Canada. Notwithstanding the submission of any such report, the Contractor remains responsible for the completion of the Work in accordance with the terms of this Contract.

(b) Such reports must include proposed detailed remedial action plans to resolve or alleviate the identified situations or difficulties. The plans must set out the Contractor's detailed estimates of any increase in time, resources and cost to effect such plans. Such plans must include all reasonable options for consideration by Canada plus the costs and consequences to Canada of taking no remedial action and must also provide a reasonable amount of time for Canada to review these options and obtain any necessary funding authorization.

(c) The Contractor is prohibited from claiming for any additional costs incurred in remedying a problem not reported as described above in a timely fashion, and is required to remedy such problems at its own expense.

7.20 Safeguarding Electronic Media

(a) Only approved USB sticks can be used on Canada's equipment. USBs that have been previously inserted into non-government furnished equipment must not be used.

(b) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

(c) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.21 Representations and Warranties

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

7.22 Access to Facilities and Equipment

Canada's facilities, equipment, documentation and personnel are not automatically at the disposal of the Contractor. If access to government premises, computer systems (micro computer network), working space, telephones, terminals, documentation and personnel for consultation is required by the Contractor to perform the Work, the Contractor must advise the Contracting Authority of the need for such access in a timely fashion. If the Contractor's request for access is approved by Canada and arrangements are made to provide access to the Contractor, the Contractor, its subcontractors, agents and employees must comply with all the conditions applicable at the Work site. The Contractor must further ensure that the facilities and equipment are used solely for the performance of the Contract.

7.23 Government Property

Canada agrees to supply the Contractor with the items listed in ANNEX A. The section of the General Conditions entitled "Government Property" also applies to the use of the Government Property by the Contractor.

7.24 Identification Protocol Responsibilities

The Contractor must ensure that each of its agents, representatives or subcontractors (hereinafter referred to as Contractor Representatives) complies with the following self-identification requirements:

(a) Contractor Representatives who attend a Government of Canada meeting (whether internal or external to Canada's offices) must identify if an individual is not a permanent employee of the Contractor prior to the commencement of the meeting, to ensure that each meeting participant is aware of the fact that the individual is not a Contractor permanent employee;

(b) During the performance of any Work at a Government of Canada site, each Contractor Representative must be clearly identified at all times as being a Contractor Representative; and

(c) If a Contractor Representative requires the use of the Government of Canada's e-mail system in the performance of the Work, t the individual must clearly identify him or herself as an agent or subcontractor of the Contractor in all electronic mail in the signature block as well as under "Properties."

This identification protocol must also be used in all other correspondence, communication, and documentation.

(d) If Canada determines that the Contractor is in breach of any obligation stated in this Article, upon written notice from Canada the Contractor must submit a written action plan describing corrective measures it will implement to eliminate the recurrence of the problem. The Contractor will have five (5) working days to deliver the action plan to the Client and the Contracting Authority, and twenty (20) working days to rectify the underlying problem.

(e) In addition to any other rights it has under the Contract, Canada may terminate the Contract for default if the corrective measures required of the Contractor described above are not met.

7.25 Non-Disclosure Agreement

The Contractor must obtain from its employee(s) or subcontractor(s) the completed and signed Non-Disclosure Agreement, attached at ANNEX D, and provide it to the Project Authority before they are given access to information by or on behalf of Canada in connection with the Work.

7.26 Time and Task Recording

The Contractor agrees that if so requested, in writing, by the Technical Authority that the Contractor must direct and ensure that its personnel report on a daily or weekly basis actual time spent carrying out work in support of specific tasks by completing time recording reports specified by Canada.

7.27 Dispute Resolution

(a) If a dispute arises out of, or in connection with this Contract, the parties agree to meet to pursue resolution through negotiation or other appropriate dispute resolution process acceptable to both parties, before resorting to litigation. All information exchanged during this meeting or any subsequent dispute resolution process, must be regarded as “without prejudice” communications for the purpose of settlement negotiations 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 will not be rendered inadmissible or non-discoverable by virtue of its use during the dispute resolution process.

(b) This clause Dispute Resolution will not affect any of Canada’s rights of cancellation or termination contained in this Contract.

7.28 Transition Services at End of Contract Period

12 months prior to the expiration of the Contract, the Contractor must prepare and provide the Technical Authority a detailed Service Transition-Out Plan. Upon acceptance of the Technical Authority, the Contractor must transition out its services to another supplier in accordance with the Plan.

7.29 Independent Verification and Validation

(a) At the sole discretion of Canada, the Technical Authority may request a review by an Independent Verification and Validation (IV & V) Team. The Contractor must provide access to the Technical Authority and Independent Verification and Verification agents. The Independent Verification and Validation process will assist the Technical Authority in the review of the Contractor's deliverable documents for;

i. Completeness, consistency and conformance to the Contract requirements; and

ii. Assessment of the level of effort to complete the Work.

(b) The Contractor must support the performance of the verification and validation services by any IV & V agents if engaged. The terms of communication are as follows:

i. the IV & V agent reports to, receives direction from and provides recommendations to only the Technical Authority, unless engaged by the Contractor;

ii. the Contractor must designate a point of contact for the IV & V agent, and I notify Canada in writing of any change; and

iii. the IV & V agen must not be required to furnish the Contractor with work plans or schedules, or with any other documentation or information.

(c) The Contractor must make available to the IV & V agen both the use of temporary workspace for a maximum of three (3) people, and access to MPM Project working materials such as documentation, software and schedules, as are normally available to the Contractor's Quality Assurance personnel.

7. 30 Integrity Provisions - Contract

The *Ineligibility and Suspension Policy* (the "Policy") and all related Directives incorporated by reference into the bid solicitation on its closing date are incorporated into, and form a binding part of, the Contract. The Contractor must comply with the provisions of the Policy and Directives, which can be found on Public Works and Government Services Canada's website at http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html.

7.31 Additional Clauses

(a) SACC Manual Clause A9068C (__-__-__), Government Site Regulations

(b) SACC Manual Clause B2008C (__-__-__), Government of Canada Web Standards

ANNEX A – STATEMENT OF WORK

TABLE OF CONTENTS

LIST OF APPENDICES:

SECTION 1: CANADA'S INDUSTRIAL SECURITY SOLUTION OVERVIEW

The portfolio of business applications that support the delivery of Industrial Security services is largely outdated and unsustainable. This shortcoming hinders the Industrial Security Sector's (ISS) efforts to meet the expectations of its Industry and Government users and partners. In order to address this problem, ISS is exploring the opportunity to modernize the technological platform that supports its operations.

The following sections provide background and context to the project being undertaken, and attempt to effectively identify constraints, assumptions and expectations.

1.1 BACKGROUND

1.1.1 Industrial Security Program

Public Works and Government Services Canada (PWGSC) is identified as one of ten Lead Security Agencies for the Government of Canada (GC). PWGSC provides leadership and coordination activities to help ensure the application of security safeguards through all phases of the contracting process within the scope of the Industrial Security Program (ISP).

PWGSC is responsible to deliver ISP services, including:

(a) Developing, based on analysis of community needs, in partnership with Treasury Board Secretariat of Canada (TBS), policy instruments, guidelines and tools related to security in contracting for approval by TBS;
(b) Coordinating the development and provision of training and awareness related to security in contracting;
(c) Leading interdepartmental committees and working groups for security in contracting to facilitate the sharing of information and collaboration across communities of practice;
(d) Collecting and reviewing best practices related to security in contracting and making recommendations to TBS and security governance committees to facilitate security policy improvements and collaboration among departments;
(e) Maintaining a database of private sector organizations and individuals that have been authorized to access classified and protected information and assets;
(f) Carrying out roles pursuant to international agreements respecting industrial security;
(g) Conducting security inspections of companies that have access to protected and classified information and assets of NATO allies or those who are registered with countries with which Canada has reciprocal Industrial Security Memoranda of Understanding;
(h) Processing requests for visits when a security cleared individual must visit a government/commercial organization in Canada or abroad;
(i) Performing the necessary security screening of private sector individuals and organizations that have access to protected and classified information and assets, including those participating in foreign contracts;
(j) Ensuring compliance in those security contracts that afford industry access to government information and assets;
(k) Controlling and managing Communications Security (COMSEC) assets in private sector companies and providing screening clearances and inspections for COMSEC assets in private sector companies; and
(l) Representing the GC on national and international initiatives related to security in contracting and controlled goods.

The ISP is delivered through the Industrial Security Sector (ISS) within the Departmental Oversight Branch (DOB) at PWGSC.

The ISS delivers two programs: the Contract Security Program (CSP) and the Controlled Goods Program (CGP). Within the CSP there are twenty-four documented processes which can be found in APPENDIX 1 to ANNEX A. Similarly, there are ten documented CGP processes that are described in detail within APPENDIX 1 to ANNEX A.

1.1.1.1 Contract Security Program

The GC's CSP provides services that are vital to Canadians and the safeguarding of information and assets that are entrusted to Canadian and international private sector organizations and their Governments. The program allows the GC to share both domestic and foreign sensitive technologies with Canadian industry as well as allowing Canadian industry the opportunity to participate in foreign classified contracts. This program maintains the trust and confidence of NATO and Canada's other allies and supports the country's anti-proliferation, public safety, security and global security priorities.

The CSP's specific functions related to contract security include:

(a) Providing personnel and facilities security screening services to Canadian private sector organizations involved in protected/classified government contracts;
(b) Inspecting organizations with access to protected and classified information/assets;
(c) Processing Canadian and foreign visit requests for visitors requiring access to program or contract-related Classified / Protected information/assets; and
(d) Transmitting program or contract-related Classified/Protected information/assets between Canadian and foreign industries and governments.

The CSP is currently operating with approximately 396 staff, all collocated in Ottawa.

1.1.1.2 Controlled Goods Program

The CGP is a registration and compliance program which regulates access to controlled goods, including *International Traffic in Arms Regulations* (ITAR) items, in Canada. The CGP plays a vital role in the prevention and detection of the unlawful examination, possession or transfer of controlled goods in Canada. Under the authorities of the *Defence Production Act* (DPA) and the *Controlled Goods Regulations*, the CGP's mandate is to strengthen Canada's defence trade controls through the mandatory registration and regulation of businesses and individuals who examine, possess and/or transfer controlled goods.

The CGP regulates approximately 4000 Canadian companies who may examine, possess or transfer controlled goods. The Program works closely with domestic security partners (Canadian Security Intelligence Service, the Royal Canadian Mounted Police, the Canadian Border Security Agency and the Global Affairs Canada) to carry security assessments for individuals or companies, to assess security risks, to provide training to Designated Officials from registered companies, to investigate and carry-out compliance-related actions.

The CGP is currently operating with approximately 91 staff, all collocated in Ottawa.

1.1.2 Industrial Security Systems Transformation Project

Business Need

ISS needs to replace its current complement of contract security and controlled goods systems with a stable, scalable, intuitive and seamlessly integrated solution. It is essential to address the experience, capacity, performance and compliance gaps that presently exist between existing ISS systems and the expectations of Industry and the GC, (e.g. system performance and stability issues, error prone, paper and manually hands on intensive file processing) which hinder the ISS in maintaining its service standards in certain areas thus impacting contract award and ultimately industry revenues. ISS must facilitate a user experience and interaction with GC that is consistent with the government's modernization objectives, while maintaining appropriate security parameters.

1.1.2.1 Project Objectives

The scope and intent of the Industrial Security Systems Transformation (ISST) project is to replace the current complement of aging systems supporting both the CSP and CGP functions within the ISS with a unified solution that better addresses the current and emerging needs of Industry and the GC. Included within the scope of the ISST project is business process re-engineering where required to align the ISS business and the proposed unified solution.

1.1.2.2 Expected Outcomes

Requirements for scalability, sustained capacity, security and stability have become essential factors in ensuring the success of PWGSC in delivering essential services on behalf of the GC. Process and solution integration, increased efficiencies, and better alignment to current program functions will allow ISS to meet and improve on service standards as well as to better monitor and inform on service requests.

The solution is to provide GC users and Industry an intuitive self-service electronic interface with the ISS. Internally, it is expected that the system will allow automated and configurable workflows managed by ISS to drive efficiencies and to not only meet performance standards but transform performance well beyond current levels. As an example, some currently published standards, which ISS expects will be improved, include:

(a) Designated organization screening: Up to six months upon receipt of a properly completed request;
(b) Facility security clearance: Six months or more upon receipt of a properly completed request and dependent on the complexity of the screening required;
(c) Reliability Status – Simple request: 7 business days upon receipt of a properly completed request;
(d) Reliability Status – Complex request: 120 business days upon receipt of a properly completed request;
(e) Classified Secret clearance request: 75 business days (in addition to reliability screening times) upon receipt of a properly completed request;
(f) CGP Registration Application: 45 days upon receipt of a properly completed request.

Successful implementation should render a number of measurable and beneficial Business Outcomes, centered on but not limited to:

(a) Increased Capacity (e.g. to register companies and to process clearances/applications);
(b) Better Service (e.g. more reliable, faster clearance/application processing);
(c) Better Information (e.g. extensive search and reporting capacity);
(d) Greater Satisfaction (e.g. user-centric, simpler, intuitive processes for Industry and other users); and
(e) Greater Efficiencies (e.g. reduced compliance costs to suppliers).

Further examples of desirable benefits/outcomes may include:

Ensure the Security and Privacy of Canadian Information and Assets	
Security	• Reduction in Security/Privacy Breaches
Achieve Better Value to Users and to Industry	
Self-Service tools	• Reduction in industry complaints
	• Reduction in receipt of incomplete forms
	• Reduction in number of inquiries for information
Streamlined Service Delivery / Reduced Process Burden	• Reduction in processing times for requests
	• Reduced times to address issues or concerns (request processing problems, client follow-up inquiries)
	• Shared tombstone data amongst the various ISS business lines
Innovative and Efficient Government	
Value for Money	• Reduction in the administration costs (paper handling, retention, destruction etc.)
Innovation	• Increased automation of work processes.
	• Elimination of the requirement for a “wet” signature.
	• Integration with existing GC solutions
Efficient Information Management	• Improved and consistent reporting
	• Reduction in the number of steps in work processes
	• Reduction in number of manual steps in work processes

2.1 NEW SOLUTION

The following diagram illustrates the high level interaction map for the required ISST Solution. Illustrated are the high level user types utilizing GC GCPass technology to access the ISST Solution's Web Portal in order to submit service requests to the ISST Solution's Service Processing Application. Alternately, users can complete forms that will populate embedded barcodes with form information and then submit those service requests for processing. Received forms will be barcode scanned to input the form information into the ISST Solution's Service Processing Application.

The ISST Solution's Service Processing Application will be used to process the submitted service requests with external to and internal government interfaces. For example, the ISST Solution will interact with the Royal Canadian Mounted Police (RCMP) to perform criminal record checks for personnel security clearance service requests. The ISST Solution will maintain a document repository, allowing remote access to CSP and CGP inspectors and investigators.

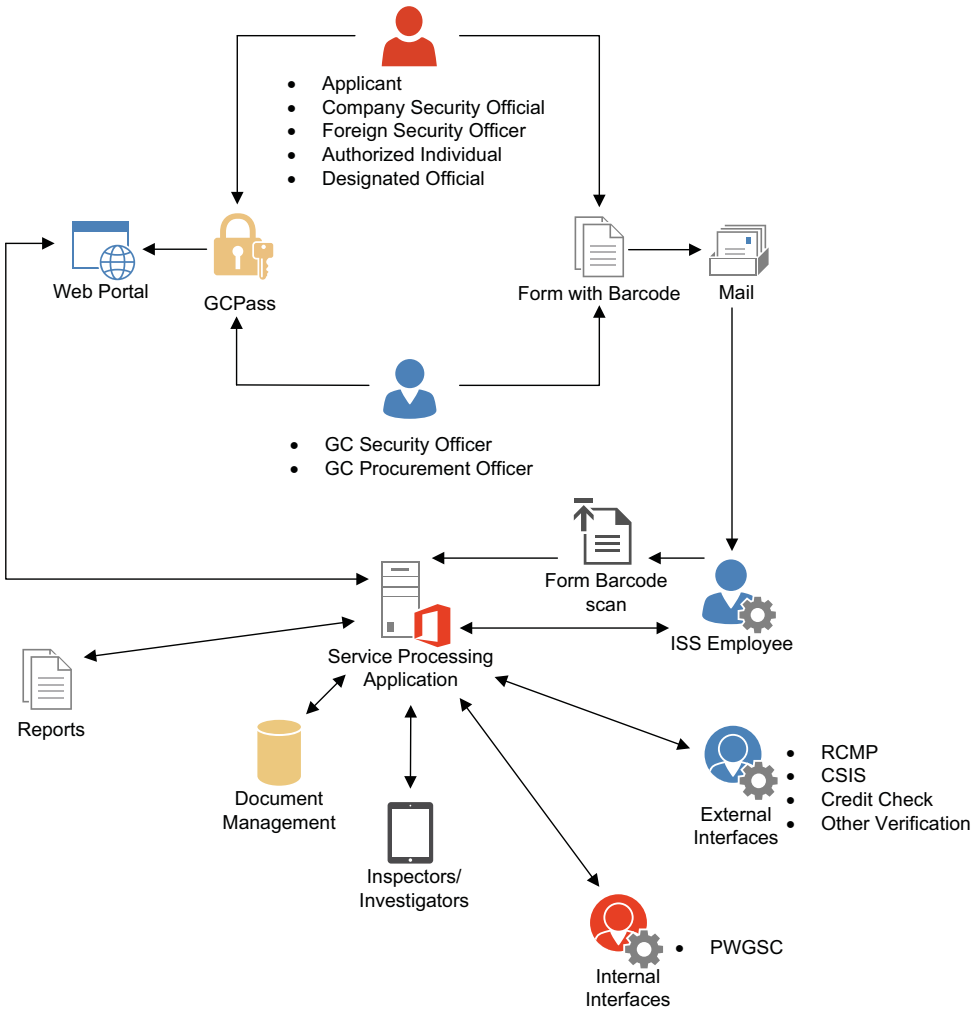


Figure 1: ISST Solution high level interaction map.

3.1 VOLUMETRIC DATA

The following volumetric data outlines volumes that the proposed solution is expected to support.

3.1.1 User Accounts

Internal Users: Current total user population of 487 accounts, of which 396 are CSP and 91 are CGP user accounts.

External Users: Current user population of 183,905 user accounts which breaks down as follows:

(a) CSP External Users - Industry: 161,000 user accounts;
(b) CSP External Users – Government Users: 905 user accounts; and
(c) CGP External Users - 22,000* user accounts.

*Note: Currently CGP does not have an External User population. However, it is estimated that the Solution will facilitate access to approximately 22,000 CGP external users

3.1.2 Activity Specific Volumes

Reported volumes are based on totals from the 2015-16 fiscal year.

CSP and CGP Registration

CSP provides registration services to Canadian organization working on GC contracts with security requirements. Currently, more than 18,400 Canadian organizations are registered in the CSP.

Registration in the CGP is legally required for any person (individuals and businesses) examining, possessing or transferring controlled goods in Canada. Currently, more than 4,500 Canadians and Canadian Businesses are registered in the CGP.

Overview of CSP and CGP Registration Activities is as shown below:

Registration Activities Overview	**CSP**		**CGP**		**Total**	
	Annually	**Daily**	**Annually**	**Daily**	**Annually**	**Daily**
New Registrations	3,438	13	454	2	3,892	15
Registrations Renewal	2,889	11	514	2	3,403	13
Amendments to Registrations	337	1	352	1	689	2
Terminations of Registration	3,124	12	306	1	3,430	13
Inspections and Investigations	5,342	20	1,804	7	7,146	27
Total Registration Activities	**15,130**	**57**	**3,430**	**13**	**18,560**	**70**

Personnel Security Screening/Clearance Requests

Employees of an organization registered in CSP who are working on a contract with security requirements are required to be security screened/cleared prior to accessing Protected and/or Classified information, assets or work sites. The CSP provides personnel security screening/clearance service to other GC organizations. Currently, there are approximately **850,000** personnel security screening/clearance files managed by CSP.

Overview of CSP Personnel Security Requests is shown as below:

Personnel Security Screening/Clearance Activities		
	Annual	Daily
Requests for Reliability Status Screening	86,907	333
Requests for Security Clearance	42,772	164
Requests for Termination	42,783	162
Close-outs	17,163	66
CGP Security Assessment Applications	1,194	6
Total Personnel Security Screening/Clearance Activities	**190,819**	**731**

Contracts Security Requests

CSP provides contracting authorities with security clauses for Government contracts, based on the security requirements of these contracts. In FY2015/2016, CSP received 10,250 (39 per day) pre-contract award service requests (SRCLs) and 9,062 (35 per day) service requests related to awarded contracts (e.g., subcontracts, contract amendments, etc.).

CSP - Visits Requests

CSP Visit Requests are required when an individual must go to a government or private organization within Canada or abroad to access sensitive information/assets as part of a government contract. In FY2015/2016, CSP logged 6,617 (25 per day) service requests for Visits.

CSP - Document Control Request

Protected and Classified information, assets and/or equipment are required to be transferred through government to government channels when entering or leaving Canada. In FY2015/2016, CSP processed 226 (1 per day) Document Control Requests.

CGP - Visitor Exemption Requests

CGP visitor exemptions are for those individuals visiting a CGP registered organization and do not required to be security assessed by the CGP. In FY2015/2016, CGP logged 1,352 (5 per day) CGP visitor exemption requests.

CGP Temporary Worker Exemption Requests

CGP temporary worker exemptions requests are for those individuals who will be temporarily working at a CGP registered organization and do not required to be registered with the CGP themselves. In FY2015/2016, CGP received 299 (1 per day) requests for Temporary Worker Exemption.

CGP - Employee Referrals Requests

Referrals are for identified high/moderate risk employees. In FY2015/2016, CGP received 23 referral service requests.

CSP and CGP – Call Center Volumes

Information inquiries made with the CSP/CGP Call Center. In FY2015/2016, the Call Center received 124,970 (479 per day) personnel security and organization verifications, and 110,331 (423 per day) inquiries.

Supporting Documentation Volumes

Page volume ranges are estimated based on typical requests to extreme case requests. To extrapolate that into size, a multiplier of 11KB (representing a single word page) as well as the provided 2015-16 fiscal year totals and approximate daily intakes were used.

Activity Area	Program	Page Min	Page Max	FY15-16 Total	FY15-16 Volume Min (GB)	FY15-16 Volume Max (GB)	FY15-16 Daily Total	FY15-16 Daily Volume Min (GB)	FY15-16 Daily Volume Max (GB)
Contracts	CSP	20	500	19312	4.1	101.3	74	0.016	0.397
Registration [1]	CSP	100	1000	9788	10.3	102.7	38	0.041	0.408
	CGP	60	100	1626	1.0	1.7	6	0.004	0.006
Inspection and Investigation [2]	CSP	100	1500	15865	16.6	249.6	61	0.066	0.983
	CGP	30	100	1804	0.6	1.9	7	0.002	0.008
Personnel Security [3]	CSP	10	100	189625	19.9	198.9	727	0.078	0.781
	CGP	20	50	1194	0.3	0.6	5	0.001	0.003
Visits	CSP	20	50	6617	1.4	3.5	25	0.005	0.013
	CGP	9	15	1352	0.1	0.2	5	0.000	0.001
Temporary Worker Exemptions and Employee Referrals	CGP	20	30	322	0.1	0.1	1	0.0002	0.0003
Document Control	CSP	20	50	226	0.1	0.1	1	0.0002	0.0005

[1] Total of new, renewal, amendment and termination registration activities.
[2] Includes inspection and investigation activities for both organizations and personnel security clearances.
[3] Total of new and termination personnel security activities.

4.1 COMMON TERMINOLOGY

Key terms and acronyms used throughout this document may be found in APPENDIX 6 to this ANNEX.

SECTION 2: BUSINESS REQUIREMENTS

This section defines the Business Process Re-Engineering and Functional requirements for the Solution.

1.1 REQUIREMENT OVERVIEW – BUSINESS PROCESS RE-ENGINEERING

The introduction of a new system represents an opportunity to revisit, rationalize, streamline and improve the delivery of ISS services. A thorough analysis of existing processes and procedures is required in order to propose leaner, faster, consolidated processes that yield tangible and measurable efficiencies.

ISS requires the development and execution of a business process reengineering strategy that will deliver measurable benefits in each of the following criteria while enhancing levels of service to industry:

(a) Reduction of process steps;
(b) Reduction of paper burden;
(c) Reduction of manual steps;
(d) Reduction in time to process; and
(e) Maximal automation of processes.

Performance measures considered will include quality and efficiency of delivered services.

ISS processes are currently heavily paper-based and require significant manual treatment. Where it is possible, it is required that ISS manual processes be substituted with system-supported functions, to dramatically reduce, if not eliminate, the requirement for paper-dependent processes.

Certain processes could potentially be fully automated. In this context, “fully automated” refers to a process that would receive a submission and execute the entirety of the remaining process, without a requirement for human intervention. One example of a possible process that can be automated is the Personnel Security Simple Reliability Screening process. It is an expectation that the full automation of (simple) Reliability Screening will form part of the Contractor’s proposed strategy and delivery. All other processes are also viable candidates for full or partial automation. See section APPENDIX 1 to ANNEX A for information regarding all of the key ISS processes, including Reliability Screening.

Effective Business Process Re-engineering is intended to:

(a) Undertake a fundamental rethinking of business processes;
(b) Streamline, consolidate and redesign business processes;
(c) Optimize end-to-end processes and automate processes;
(d) Remove, replace or consolidate processes that do not add business value; and
(e) Address stakeholder expectations in the areas of Innovation, Responsiveness, Speed, Quality and Service.

The Contractor must ensure the co-ordination of the Business Process Re-engineering Plan and activities and all other project activities, in accordance with the Project Management Plan and Project Schedule.

1.2 DETAILED REQUIREMENTS – BUSINESS PROCESS RE-ENGINEERING

The Contractor must:

Category	SOW NUM	Requirement
Business Process Re-Engineering	BR.01	Prepare a Business Process Re-engineering Plan which includes, but is not limited to: (a) Elaborating on objectives for business process re-engineering as it relates to the ISST Solution; (b) Strategic purpose of business process re-engineering as part of the ISST Solution; (c) Expand on how the business process re-engineering gap analysis will be conducted; and (d) Elaborate on how the constraints and impacts will be addressed as a result of the business processing re-engineering; and (e) Provide details on the scheduling of business process re-engineering activities.
	BR.02	Conduct a detailed analysis of current As-Is business processes, service request forms, workflows and associated business rules.
	BR.03	Develop a Business Process Re-engineering Proposal, identifying proposed process models, underscoring significant changes, and including elaboration of value-adding processes and expected outcomes.
	BR.04	Design To-Be processes, workflows, service request forms, solution functions and develop business process maps.
	BR.05	Create where required new service request forms for inclusion within the Solution to facilitate electronic capturing of process information. For example, currently there is no service request form for the registration of an organization with the CSP.
	BR.06	Where possible, propose and modify existing service request forms to facilitate the capturing and processing of service request. For example, the CGP registration forms can be updated if required. Note that the forms utilized for the personnel security clearance screening are developed by TBS and may not be available for modification.
	BR.07	Perform a Gap Analysis to identify areas (business processes and users as a result of the process re-engineering) for future Change Management engagement.
	BR.08	Determine appropriate measures to identify success and develop benchmark performance measurement criteria which will be used later as part of the operational readiness assessment.
	BR.09	Develop the business architecture for the solution.
	BR.10	Conduct a simulation analysis of options to determine optimal improvements.

Category	SOW NUM	Requirement
	BR.11	Demonstrate business process re-engineering success by completing an identified process from start to finish that touches on all the major areas functionalities as identified by the requirements in the detailed business requirements contained within ANNEX A (ANNEX A, Section 2). The identified process will be selected by the Contractor after completion of their gap analysis and business process re-engineering activities.
	BR.12	Incorporate and implement approved To-Be processes and workflows into the solution design.
	BR.13	Risks identified during the business process re-engineering must be incorporated into the project Risk Register (ANNEX A, Section 7).
	BR.14	Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues.
	BR.15	Provide updated Status Report and Risk Register monthly.
	BR.16	Develop re-engineered process oriented end-to-end standard operating procedures outlining key activities and user responsibility so that end users are informed as to how the business process re-engineering impacts their day to day activities.
	BR.17	Co-ordinate Business Process Re-engineering activities to required Change Management activities to facilitate successful adoption of the Solution.
	BR.18	Deliver a Business Process Re-engineering Report describing the entire Business Process Re-engineering process undertaken, the results of analysis, the To-Be design, the efficiencies and benefits to be realized, the measurement criteria to be applied, Change Management Plan linkages and lessons learned. The Business Process Re-engineering Report is subject to Project Authority review and approval.

2.1 REQUIREMENT OVERVIEW – FUNCTIONAL REQUIREMENTS

The Solution is a business application composed of two major components: a Service Processing Application and a Web Portal.

The Service Processing Application is the portion of the complete Solution that will support the processing of ISS service requests. The Contractor must deliver a Solution with a Service Processing Application that:

(a) Supports the achievement of higher operational efficiencies through the streamlining and automation of partial or entire ISS business processes;
(b) Provides a user friendly interface that promotes efficient service processing;
(c) Enables Internal Users to communicate effectively with External Users and entities;
(d) Enables Internal Users to efficiently manage a case file throughout its life cycle;
(e) Supports and maintains a high quality of case file related data and their relationships;
(f) Supports embedded validation mechanisms to ensure data and processing completeness and accuracy;
(g) Supports the GC greening agenda by replacing paper based workflows and processes;
(h) Supports remote access of case files;
(i) Enables the acquisition, storage and the communication of supporting information (supporting documents and correspondence) in electronic formats;
(j) Interfaces with other GC applications and Enables interconnectivity with external agencies;
(k) Facilitates standard reporting on ISS business activities and trends through a suite of available reports; and
(l) A Solution that implements the core services rendered by the ISS;

The Web Portal is the public-facing internet-based information exchange component of the Solution that will serve as the central, enabling, self-service interface enabling communication and interaction between External Users and the two Industrial Security Sector programs: Contracts Security Program and Controlled Goods Program. The Contractor must deliver a Solution with a Web Portal that:

(a) Provides a secure single point of access to ISS services;
(b) Enables External Users the ability to self-manage aspects of their service requests and user profiles;
(c) Enables External Users to configure their self-services portfolio based on preferences (e.g. favourites, etc.);
(d) Enables External Users to access ISS services without requiring direct interaction with an ISS representative or specific training;
(e) Provides a single point of communication with ISS to enable them to access general information and exchange with ISS information related to their service requests, in an efficient, secure and timely manner;
(f) Provides External Users with enhanced Mobility/Accessibility;
(g) Provides External Users with an alternate means to submit requests to the ISS;
(h) Has the capacity to increase the solution's user base by multiple orders of magnitude without decreasing the level of service provided;
(i) Enables high accuracy of data acquisition; and
(j) Ensures External User transaction response in near real-time.

A component of moving from the current legacy systems to the new solution will be the migration of identified data. Data migration planning, development, and validation must be completed by the Contractor using a controlled sample size of the data that covers the various data types and elements currently stored. While the Contractor is expected to plan for the data migration, the Contractor will not be required to perform the actual

data migration. It is expected that PWGSC CIOB/SSC will perform the data migration following the data migration strategy and plan developed by the Contractor.

2.2 DETAILED REQUIREMENTS – FUNCTIONAL REQUIREMENTS

2.2.1 Service Processing Application

The Contractor must deliver a Service Processing Application that provides the following functionalities, but is not limited to:

Category	SOW NUM	Requirement
Automation	APP-AU.01	Enables the automation, of ISS business processes. For example simple reliability personnel security clearance or clearance duplication requests must be fully automated if all request validation criteria are satisfied upon submission by the External User. See APPENDIX 1 to ANNEX A for details on the simple reliability or duplication processes.
	APP-AU.02	The automatic issuing of appropriate approval certificates (e.g. personnel screening briefing certificate): (a) For service request satisfying all identified mandatory criteria (e.g. security partner verifications); (b) Notification sent to External User indicating that their service request was approved; (c) Generation of appropriate approval certificate with corresponding signatures and validation dates of the request; and (d) Availability of appropriate approval certificate to the External User for download/printing from the Web Portal.
	APP-AU.03	Automatic management of user accounts: (a) Automatically generates accounts for External User of type Applicant when requested by External User of type Security Official or Designated Official, this is in conjunction with requirement *WP-UE.01*; (b) Automatically disables accounts for External Users of type Applicant upon completion of associated Personnel Security Screening Request, or after a predefined period of inactivity; (c) Automatically disables accounts belonging to organizations that are no longer registered (or terminated) with the ISS; and (d) Automatically deletes all disabled accounts after a predefined period of time.
	APP-AU.04	Automatic population of the External User's web portal calendar feature with pre-defined events relating to service requests submitted to ISS (e.g. correspondence due dates, organizational registration renewals, etc.).

Category	SOW NUM	Requirement
Operations Support	APP-OPS.01	Enforces a Role Based Access Control over all defined users and objects.
	APP-OPS.02	Enables Internal Users with appropriate permissions the ability to add, modify, disable or delete External and Internal User accounts.
	APP-OPS.03	Enables Internal Users with appropriate permissions the ability to add, modify, delete or disable Internal and External User account capabilities or assigned roles.
	APP-OPS.04	Enables Internal Users with appropriate permissions the ability to add, modify, delete or disable assignable user roles within the solution.
	APP-OPS.05	Enables Internal Users with appropriate permissions the ability to add, modify, delete or disable the capabilities assigned to a user role.
	APP-OPS.06	Enables Internal Users with appropriate permissions the ability add, modify, delete or disable capabilities that are available for assignment to a user role or user.
	APP-OPS.07	Enables Internal Users with appropriate permissions the flexibility and adaptability in the implementation of future policies and business rules/processes as well as the modification of existing business rules/processes utilized by the solution as a whole, i.e., both the external facing web portal and internal processing application. For example, to be able to modify the solution parameter defining the standard number of days to completed a CGP registration request. This is then automatically reflected on all reports and dashboards and used in all internal calculations.
	APP-OPS.08	Enables Internal Users with appropriate permissions the flexibility and adaptability to add, modify, delete or disable workflows within the solution.
	APP-OPS.09	Enable Internal Users with appropriate permissions to maintain business forms for case processing, i.e., privileged users can add new data fields to forms to capture additional information. Likewise, to disable existing data fields if no longer required.
	APP-OPS.10	Enables Internal Users with appropriate permissions to modify externally facing forms and publish them to the web portal.
	APP-OPS.11	Enables Internal Users with appropriate permissions the ability add, modify, delete or disable whole or parts of Solution used templates (e.g. correspondence templates, etc.).
	APP-OPS.12	Enables Internal Users with appropriate permissions to modify system produced certificates, for example, Personnel Security Screening Certificate, Controlled Goods Registration Certificate, etc.
	APP-OPS.13	Enable automated tracking of cases as they progress through the various process/workflow stages (e.g. progress bars, percentage and time to completion).

Category	SOW NUM	Requirement
	APP-OPS.14	Enable automated tracking of external inquiries/service tickets submitted to the ISS as they progress through the various stages (e.g. progress bars, percentage and time to completion).
	APP-OPS.15	Enable automated triage and triggering of service requests to optimize request processing (only exceptions will require manual intervention). For example, upon receipt of a service request and based on its type, the request could be automatically triaged based on inputted data and assigned to a specified processing team (e.g. simple reliability vs classified personnel security clearances). As another example, once a certain processing action has been completed the service request could be automatically assigned to the next processor to continue the movement of the request (e.g. Triggering of an inspection activity once the organization and personnel have been cleared).
	APP-OPS.16	Enable automated grouping of compliance cases based on location to facilitate work load assignment and processing.
	APP-OPS.17	Enable automated categorization based on risk or when a follow-up action is required to facilitate processing and to avoid unnecessary delays.
	APP-OPS.18	Enable automated prioritization of service requests based on predetermined operational priorities or assessed industry requirements (e.g. an urgent NATO security clearance request that requires priority processing).
	APP-OPS.19	Enables Internal users with appropriate permissions to clone a read only service request that is in progress to assist with inquires and application completion. The cloned service request should display the same as what the External User would see via the web portal. This is to allow the Internal User to see what the External User is seeing on screen and vice versa.
	APP-OPS.20	Enables Internal Users with appropriate permissions the ability to maintain access control and permissions at the field level at the user role level. For example, a field may have write access for one user role, but be read only for another user role. In another case the field may not be visible for a particular user role. Field level permissions should always be most restrictive.
	APP-OPS.21	Enables Internal Users with appropriate permissions to, on demand, update a sandbox environment with a copy of the solution from production for the purpose of refreshing the sandbox environment.
	APP-OPS.22	Enables Internal Users with appropriate permissions to enable and disable a link that External User can access from the Solution Web Portal to gain access to the Sandbox/Training environment. See business requirement *WP-UE.22*.

Category	SOW NUM	Requirement
	APP-OPS.23	Enables Internal Users with appropriate permissions to access, modify and provide access to the various environments that will be implemented over the course of the ISST. The purpose would be for implementation of future business changes, testing of future business changes, release of future business changes to a pre-production environment for release preparation, migration of tested/accepted business changes into production, etc. These solution environments include, but are not limited to: (a) Development; (b) Testing; (c) User Acceptance Testing; (d) Staging; and (e) Production.
	APP-OPS.24	Enables versioning configurations, and enables the ability to roll back to a previous version of sections of the Solution, not the whole solution, if a released change is creating an issue in said section. Such a feature would be limited to Internal Users with appropriate permissions.
User Experience	APP-UE.01	Enables Internal Users to access or navigate across multiple workflows and cases.
	APP-UE.02	Provides Internal User assistance embedded within the Solution via features such as context sensitive hover features, on screen user interactive objects, standard operating procedures as well as clear and concise system messages, etc. As an example, if an Internal User holds the mouse over a form field, contextual help is displayed to assist the user.
	APP-UE.03	Enables a synchronous calendar system that will notify the Internal Users of predefined events relating to service requests received (e.g. correspondence due dates, inspections schedule, etc.).
	APP-UE.04	Supports at minimum 1000 concurrent Internal Users.
	APP-UE.05	Provides support for content navigation.
	APP-UE.06	Provides access to Application Internal User interfaces in the user's Official Language of choice.
	APP-UE.07	Delivers, enables and supports the ability to permit all Internal Users to select their default language of operation as part of their profile. (a) This selection must include English and French interfaces; and (b) This selection must provide to the user an English or French User Interface to the solution at the choice of the user.
	APP-UE.08	Delivers, enables and supports the ability to store, manage and present information, data, metadata, and content in both Canadian Official Languages.
Information Management	APP-IM.01	Enables Internal Users to access supporting documents stored within the Solution, according to their operational requirements and authorization (Role Based Access Control).
	APP-IM.02	Enables Internal Users to manage supporting documents throughout a case lifecycle, according to their granted privileges.
	APP-IM.03	Protects evidence documents from unauthorized access, modification or deletion.

Category	SOW NUM	Requirement
	APP-IM.04	Provides Internal Users with the least amount and types of system privileges that still provides them with an unimpeded ability to perform their jobs.
	APP-IM.05	Limits document access to users having a need-to-know, the proper personnel security clearance or reliability status, and the proper authorization.
	APP-IM.06	Enables Internal Users to vet the pertinence of a supporting document to a specific case and determine appropriate action to be taken (append to case, delete, etc.).
	APP-IM.07	Enables Internal Users to associate a document to one or more cases.
	APP-IM.08	Enables Internal Users to search information (data elements) across multiple workflows and cases.
	APP-IM.09	Enables Internal Users with appropriate permissions to search supporting documents stored within the Solution.
	APP-IM.10	Enables the storage of all correspondence (e.g., emails, notifications) between Internal and External Users associated to a case, and enable the Internal User to reference all case correspondence in decision making.
	APP-IM.11	Enables Internal Users to establish relationships between cases based on specific data elements or content. For example, a cross reference between one case and one or more other cases by Organization ID. This capability will complement automated data rationalization.
	APP-IM.12	Enables Internal Users to close (terminate) a case at any point during its lifecycle.
	APP-IM.13	Enables data and information acquisition throughout a case lifecycle (e.g. an organization's security request for Document Safeguarding Capability will require acknowledgment of compliance before the security clearance can be granted).
	APP-IM.14	Facilitates the assignment, reassignment and redistribution of case files based on available resources, case priority or case complexity (which is complementary to automated workflows).
	APP-IM.15	Facilitates collaboration throughout ISS business lines by allowing Internal Users to create notes containing free text and associating them with users, cases, supporting documents, location or events at any point during the workflow.
	APP-IM.16	Enables and supports case file archiving.
	APP-IM.17	Provides a single data repository that supports all aspects of the services provided by the ISS.
	APP-IM.18	Ensures the quality of all data through the use of validation tools (e.g. global address validation).
	APP-IM.19	Facilitates the resolution and standardization of date and time to a common format to enable accurate performance measurement.
	APP-IM.20	Enables the sharing of common data elements between ISS programs as well as other information systems for data federation.
	APP-IM.21	Supports a user defined data dictionary or centralized repository of information containing data meaning, relationship to other data, origin, usage and format.
	APP-IM.22	Facilitates common identifiers across the various ISS business lines and must facilitate the use of common data elements across service requests.

Category	SOW NUM	Requirement
	APP-IM.23	Enables the display and printing of form versions from which the original service request was submitted.
	APP-IM.24	Enables correspondence exchange, enable scheduling and tracking of appointments as related to case file processing requirements.
	APP-IM.25	Facilitates the ability to store and manage case related structured and unstructured data.
	APP-IM.26	Enables Internal Users with appropriate permissions to make any required modification to case file data (e.g. add, delete, modify, reload, etc.) while maintaining the integrity of information.
	APP-IM.27	Enables Internal Users to retrieve archived records from a case file for a specified period of time.
	APP-IM.28	Provides access to all historical evidence documents within the Solution (e.g. all digitized documents that are stored on the Matane Document Imaging Solution).
	APP-IM.29	Ensures that all information in transit between IT systems and at rest is encrypted with CSE approved encryption mechanisms.
Communication	APP-COM.01	Enables automatically generated internal and external notifications based on specified actions performed on the request (e.g., once an organization's inspection has been completed, the registration officer assigned to the case is notified to finalize the organization's registration).
	APP-COM.02	Enables automatic notifications of the appropriate internal decision maker when a decision is required. Likewise, once a decision has been taken, affected Internal and External Users must be notified.
	APP-COM.03	Enables External Users to automatically receive standardized text notifications resulting from predefined events such as decision made regarding the service request.
	APP-COM.04	Preserves a record of all correspondence (content included) related to a service request.
	APP-COM.05	Enables Internal Users the ability to disseminate customized messages to targeted groups of External Users (e.g., foreign Designated Security Authorities can be contacted for foreign clearance assurance).
	APP-COM.06	Enables Internal Users the ability to generate and print correspondence that will be sent via postal services (e.g. issuing of authorization code for first time authentication into the web portal to CGD Authorized Individuals).
	APP-COM.07	Assists in request routing and workload scheduling through internal user notifications.
Paperless	APP-PPL.01	Enables the acquisition, storage and the communication of supporting information (supporting documents and correspondence) in electronic formats and are associated/attached to the case file.
	APP-PPL.02	Enables the scanning of paper documents for appendage to case files.

Category	SOW NUM	Requirement
	APP-PPL.03	Enables Internal Users to input service request information into the Solution's Service Processing Application through the scanning of form embedded barcodes (this is to complement the web portal functions for service requests submitted through alternative communication channels (e.g. mail); In addition, this will eliminate the need for manual data entry of information captured on submitted service request forms).
	APP-PPL.04	Enables Internal Users to use parts of the Solution offline (e.g. an ISS inspector will be able to reserve a case file (including associated documents), process information offline at the inspection site and synchronize the reserved case file when connectivity is available).
	APP-PPL.05	Enables Internal Users to append information to case files in a variety of formats including images, video, sound, etc. (e.g., during a compliance inspection, the inspector will be able to take pictures or record video and append them directly to the case).
Interconnectivity	APP-ICN.01	Interfaces with the SABA learning software for the delivery and tracking of training requirements. The solution is required to feed the SABA environment with user account information so that External and Internal Users can access SABA for training purposes. Upon completion of required training, SABA must be able to provide an update to the Solution with a record of completed training such that service requests can be processed. For example, within the CGP, Designated Officials (DO) are required to complete mandatory training and certification before the company's application to register with the CGP can be approved.
	APP-ICN.02	Interfaces with PWGSC's E-Procurement Solution (if and when available).
	APP-ICN.03	Interfaces with Receiver General electronic payment solution, RGBB (if and when available).
	APP-ICN.04	Interfaces with the received RCMP Criminal Record Check Fingerprint results for the purpose of matching a submitted service request to corresponding fingerprints and their results. The match is completed via a unique Document Control Number that is provided to the applicant by the RCMP and is required as part of the information submitted with the service request. This must occur automatically on successful submission of the service request from the web portal into the processing application. It must also available as an option to be triggered by Internal Users on demand.
	APP-ICN.05	Interfaces with the RCMP for Law Enforcement Record Checks (LERC). This must be available on an on demand basis. In other words, the solution must be able to submit to the RCMP the required information to perform the LERC, accept the LERC response back from the RCMP and to incorporate the LERC response into the solution for continued processing/decision making. This must occur as a result of a manual action by an Internal User as required. The submission to the RCMP and receipt of the response must be seamless and transparent to the Internal User.

Category	SOW NUM	Requirement
	APP-ICN.06	Interfaces with the RCMP to allow the RCMP to send updated security information on an as and when required basis.
	APP-ICN.07	Interfaces with CSIS for a CSIS loyalty assessment. This must be available on an on demand basis. In other words, the solution must be able to submit to CSIS the required information to perform the CSIS loyalty assessment, accept the loyalty assessment response from CSIS and incorporate the response into the solution for continued processing/decision making. This must occur as an automated process for those service requests that require a CSIS loyalty assessment (e.g. Secret personal security clearance). This must also be available to be manually triggered by an Internal User as required. The submission to CSIS and receipt of response must be seamless and transparent to the Internal User.
	APP-ICN.08	Interfaces with credit bureau(s) for the purpose of performing a financial inquiry on individuals. The solution must be able to submit to a financial inquiry service provider the required information so that the provider can perform the financial inquiry, accept the financial inquiry response and incorporate the response information into the solution for continued processing/decision making. This must occur as an automated process for those service requests that require a financial inquiry. This must also be available to be manually triggered by an Internal User as required. The submission to the credit bureau(s) and receipt of response must be seamless and transparent to the Internal User.
	APP-ICN.09	Interfaces with an Address Validation Provider for the purpose of performing address validation.
	APP-ICN.10	Interfaces with DND's Director Foreign Liaison System (DFL3) for the receipt of US to Canada and Foreign to Canada visit requests. Note that this requirement may change to become a requirement to interface with the US Department of Defence, Defence Security Service System (DSS). If possible.
Reporting and Analysis	APP-RP.01	Enables Internal Users to generate reports for tracking, measurement and reporting of performances (e.g. actual performance vs planned performance as well as performance against user defined industry and government indicators).
	APP-RP.02	Enables Internal Users to generate reports that provide management with information to support decisions.
	APP-RP.03	Enables Internal Users to generate standard reports that enable the users to monitor individual workloads.
	APP-RP.04	Enables Internal Users to generate summary reports that count totals of a target subject based off set criteria. E.g. Total number of ISS Call Centre logs for a specified date range that is then broken down into various categories such as Log Status, Log Type, Log Category, Inquires per Directorate, etc.
	APP-RP.05	Enables Internal Users to generate reports that target a specific subject and provides calculative numbers based off set criteria. E.g. Percentages of completed personnel clearance request within in standard for a specified date range.
	APP-RP.06	Enables Internal Users to generate customized and comprehensive reports based on user selected criteria. E.g. List of registered organizations and their contact information within the CGP that are located with British Columbia.

Category	SOW NUM	Requirement
	APP-RP.07	Enables Internal Users to generate reports that takes multiple targets or summaries from other reports to provide an analytic to educate. E.g. Number of CGD registration requests completed within target for each year for the last five years, indicating percentage of increase or decrease in activity over the same reporting period.
	APP-RP.08	Enables Internal Users to generate reports that shows information on a particular subject based on selected criteria that shows historical documentation of activities to completion. E.g. Processing history of a specified personnel clearance file.
	APP-RP.09	Enables Internal Users with appropriate permissions to add, modify, enable, disable, delete, promote or demote solution reports as required.
	APP-RP.10	Enables Internal Users to generate any reports associated to the Solution without consulting other partners.
	APP-RP.11	Enables Internal Users to define query reports and save them for repeated use.
	APP-RP.12	Enables Internal Users to promote or demote reports from a query status to standard reports status. Thus allowing them to be included as part of the solutions suite of standard reports externally (web portal) and internally (processing application).
	APP-RP.13	Enables Internal Users to modify the selection criteria associated to a report. For example, the user should be enabled to add or remove selection criteria.
	APP-RP.14	Enable Internal Users to modify the selection criteria associated to the standardized reports that is available to External Users on the web portal.
	APP-RP.15	Enable Internal Users to control access to solution available reports based on user access role and permissions. E.g. A solution available report that is specifically designed for the CGP Investigation and Analysis Unit should only be available to that user role. Should the need arise, access to that report could be shared with other user roles.
Process Implementation	APP-PI.01	Enables the implementation of ISS Business Processes, including but not limited to: (a) Personnel Security Screening Services; (b) Organization Registration Services; (c) Inspections and Investigations Services; (d) Contract Security Services (including Visit and Document Control requests); (e) Controlled Good Services; and (f) User Outreach Services.
	APP-PI.02	Includes a Business Requirements Document - Detailed requirements with traceability matrix aligning the high level requirements with the detailed requirements.

2.2.2 Web Portal

The Contractor must deliver a Web Portal that provides the following functionalities, but is not limited to:

Category	SOW NUM	Requirement
Service Hub	WP-SH.01	Enables secure access for External Users at logon.
	WP-SH.02	Uses approved government methods for user identification and authentication (e.g. GCPass, GCKey, MyKey, etc.).
	WP-SH.03	Supports at minimum 1000 concurrent External Users.
	WP-SH.04	Maintains service quality and performance as the user base expands over time, in particular, with respect to requirements *WP-SH.05, WP-SH.06, WP-SH.10, WP-SH.11, WP-SH.12, WP-UE.04, WP-UE.05, WP-UE.06, WP-UE.07* and *WP-UE.08.* (i.e., the Solution must not experience any increased delays, unexpected time-outs, or loss of saved information).
	WP-SH.05	Enables a synchronous exchange of information between the Web Portal and the Services Processing Application.
	WP-SH.06	Enables External Users to submit and manage service requests, including but not limited to: (a) Complete service request forms; (b) Save and revisit incomplete forms; and (c) Submit completed forms.
	WP-SH.07	Enables External Users to upload (submit) electronic documents in support of their service requests (e.g. Copy of passport, building plans, etc.).
	WP-SH.08	Performs comprehensive data validation ensuring all required data elements are completed prior to service request submission.
	WP-SH.09	Prevents External Users from submitting incomplete service requests.
	WP-SH.10	Enables External Users to manage changes to their service requests (e.g. service request cancelation, update to information, etc.).
	WP-SH.11	Enables External Users to view the status of service requests, including but not limited to: (a) View completed milestones/activities; (b) View pending milestones/activities; and (c) View estimated completion timeline.

Category	SOW NUM	Requirement
	WP-SH.12	Enables External Users to search/access historical information related to past service requests.
	WP-SH.13	Enables External Users to update their user profiles.
	WP-SH.14	Enables access to approved service request outputs, (e.g. personnel security briefing certificates) for download by External Users.
	WP-SH.15	Enables External Users to view and download service request forms, guidelines, manuals, etc.
	WP-SH.16	Enables External Users to view the status of submitted service requests, service inquiries and service tickets.
	WP-SH.17	Enables External Users to customize their interactions with ISS according to their preferences.
Communications Hub	WP-CH.01	Enables External Users to receive general and personalized notifications as their service request is processed.
	WP-CH.02	Enables External Users to send/receive messages to/from ISS.
	WP-CH.03	Enables External Users to download documents as a result of their service requests (e.g., training certificate, security clauses for contracts, etc.).
	WP-CH.04	Provides user assistance embedded within the web content via features such as context sensitive hover, on screen user interactive objects, links to manuals, FAQs, clear and concise system messages, etc.
	WP-CH.05	Includes a synchronous calendar system that will notify the External User of pre-defined events relating to service requests submitted to ISS (e.g. correspondence due dates, organizational registration renewals, etc.).
	WP-CH.06	Enables External Users of type “Security Official” to forward notifications received from the ISS directly to the End Users of type “Applicant”.
	WP-CH.07	Enables External Users of type “Applicant” to send notifications only to End Users of type “Security Official” who requested the creation of their account.
	WP-CH.08	Provides External Users with the ability to submit a service inquiry/service ticket to the ISS. (E.g. Follow-up inquiry looking to see why a personnel clearance has not progressed after a given amount of time).
User Experience	WP-UE.01	Enables authorized External Users to request the creation of accounts for other External Users (e.g., a Security Official must be able to request the creation of an account for an individual (Applicant), to complete a request).
	WP-UE.02	Enables authorized External Users to complete service requests, electronically sign the requests and then submit them to other External Users for review and approval, prior to submission to the ISS (e.g., an Applicant must be able to complete a request and then mark it as signed, at which point the Security Official will receive the Request for review and submission to the ISS for processing).
	WP-UE.03	Enables authorized External Users (e.g. Security Official) to complete service requests on behalf of other External Users (e.g. Applicant). For example, a Security Official completes a Personnel Security Screening Request on behalf of an Applicant. The Applicant is required to sign the form before the CSO can sign the form for submission.

Category	SOW NUM	Requirement
	WP-UE.04	Enables authorized External Users (e.g. Security Official) the ability to forward service requests that were completed on behalf of another External User (e.g. Applicant) for review and electronic signature.
	WP-UE.05	Enables External Users to use common mobile devices that are equipped for Internet browsing to access the web portal at any time using any device. This includes electronic signatures.
	WP-UE.06	Enables External Users to access the web portal from tablets equipped with Internet browser, without any loss of portal functionalities.
	WP-UE.07	Enables External Users to access an abridged version of the web portal from smartphones.
	WP-UE.08	Enables External Users to receive system wide notifications such as services interruptions, etc.
	WP-UE.09	Enables External Users to receive SMS standardized messages pertaining to service request updates.
	WP-UE.10	Provides access to Service request forms in an alternate format that the External User can download and complete outside of the Web Portal and submit to the ISS for processing.
	WP-UE.11	Provides access to downloadable fillable forms that must contain similar data validation capabilities as their online counterparts where possible.
	WP-UE.12	Provides access to alternate format service request forms that must provide a means by which form inputted data is captured into a barcode that can be transferred into the solution without manual entry, (e.g. barcode scanning) in correlation with *APP-PPL.01, APP-PPL.02* and *APP-PPL.03.*
	WP-UE.13	Ensures high accuracy through the use of data validation tools (e.g. global address validation, etc.) and through data federation with various government partners.
	WP-UE.14	Prevents External Users from submitting a duplicate service request for a request that is already in process or has been completed. E.g., External Users should not be able to submit another new secret security request if a valid one already exists.
	WP-UE.15	Provides flexibility and adaptability in the implementation of future policies and business rules/processes.
	WP-UE.16	Enables External Users to sign their service requests with an electronic signature.
	WP-UE.17	Enables External Users to navigate throughout the web portal in a manner that is consistent with the GC Web Standards.
	WP-UE.18	Enables External Users to set the priority of their service request with provided justification to be assessed during processing activities.
	WP-UE.19	Enables External Users to create additional requests from inputted information, whereas only the delta is required. For example, if an individual has already submitted an application for a personnel security reliability clearance and later wishes to apply for a secret clearance, the individual should only have to supply the information to make up the secret application and not have to re-enter the information that was supplied as part of the reliability clearance request.
	WP-UE.20	Enables External Users to save their submitted forms to PDF format such that is resembles the actual service request form.

Category	SOW NUM	Requirement
	WP-UE.21	Provides form validation as each section is completed with clear and concise message to alert the External User to potential errors.
	WP-UE.22	External User Training Environment: Enables External Users to access a separate public facing training environment or sandbox environment for the purpose of learning about and gaining exposure to the services provided by the ISS. This training environment must only display web portal functionalities and not retain or transmit any data during the course of its usage.
	WP-UE.23	Delivers, enables and supports the ability to store, manage and present information, data, metadata, and content in both Canadian Official Languages.
	WP-UE.24	Delivers, enables and supports the ability to permit all External Users to select their default language of operation as part of their profile. (a) This selection must include English and French interfaces; and (b) This selection must provide to the user an English or French User Interface to the solution at the choice of the user.
	WP-UE.25	Language Preference: Application External User interfaces must be available and presented in the user's Official Language of choice.
Reporting and Analysis	WP-RP.01	Usage Reporting: Provides the ability to collect and report on usage information according to GC standards.
	WP-RP.02	Enables External Users to produce standardized reports based on a limited set of pre-defined criteria. For example, a report that allows the Security Official the ability to see the status of all personnel security clearance submissions for their organization with filtering criteria that allows for selection between a specified date range and all submissions or for a specific applicant.
	WP-RP.03	Provides access to available reports in PDF, Excel (XLS, XLSX) and Word (DOC, DOCX) formats for download and printing by External Users.
	WP-RP.04	Enables External Users to save or print the reports on demand.

2.2.3 Data Migration

The Contractor must perform and deliver on the following data migration activities:

Category	SOW NUM	Requirement
Data Migration	APP-DM.01	Develop a Data Migration strategy which includes key considerations and provides recommendations on the approach to data migration activities. Note that the Contractor will not be performing the final data migration, this will be performed by PWGSC CIOB/SSC.

Category	SOW NUM	Requirement
	APP-DM.02	Develop a Data Migration Plan which includes: (a) A detailed description of all activities required to complete Data Migration from the legacy systems to the Solution, including: i. Data analysis; ii. Migration tools development/configuration; iii. Migration testing; iv. Data migration validation; and v. Data migration documentation. (b) A proposed schedule for completion of all described Data Migration activities. The proposed schedule must respect the timelines identified within the Project Schedule. (c) An estimate of number and categories of resources required to complete each migration activity and a breakdown of associated costs.
	APP-DM.03	Document a mapping of all data requiring migration to the new architectural design. Mapping documentation must be kept up to date in the event that the system architecture changes.
	APP-DM.04	Execute a migration of sample data and perform data validation to assess integrity of data and impacts of migration to new system. The sample of data must include 50 records from each process, e.g. personnel security screening, controlled goods, etc. Report findings to Project Authority, indicating level of success of migration approach.
	APP-DM.05	Document all required steps to implement the Data Migration Plan. Maintain documents up to date in the event that system architecture changes.

SECTION 3: TECHNICAL REQUIREMENTS

This section defines the technical requirements for the Solution.

1.1 REQUIREMENT OVERVIEW

The Contractor must design, develop, configure, test, implement, deploy and stabilize to a steady state, the Solution as illustrated in Figure 2 below. The Solution must accommodate the modification, adjustment, or addition of business process workflows, system automated functions, and other related rules and processes with minimal application code changes. The Solution must be user friendly, reliable, maintainable, scalable, interoperable, and compliant with GC IT/IM policies, guidelines and environment.

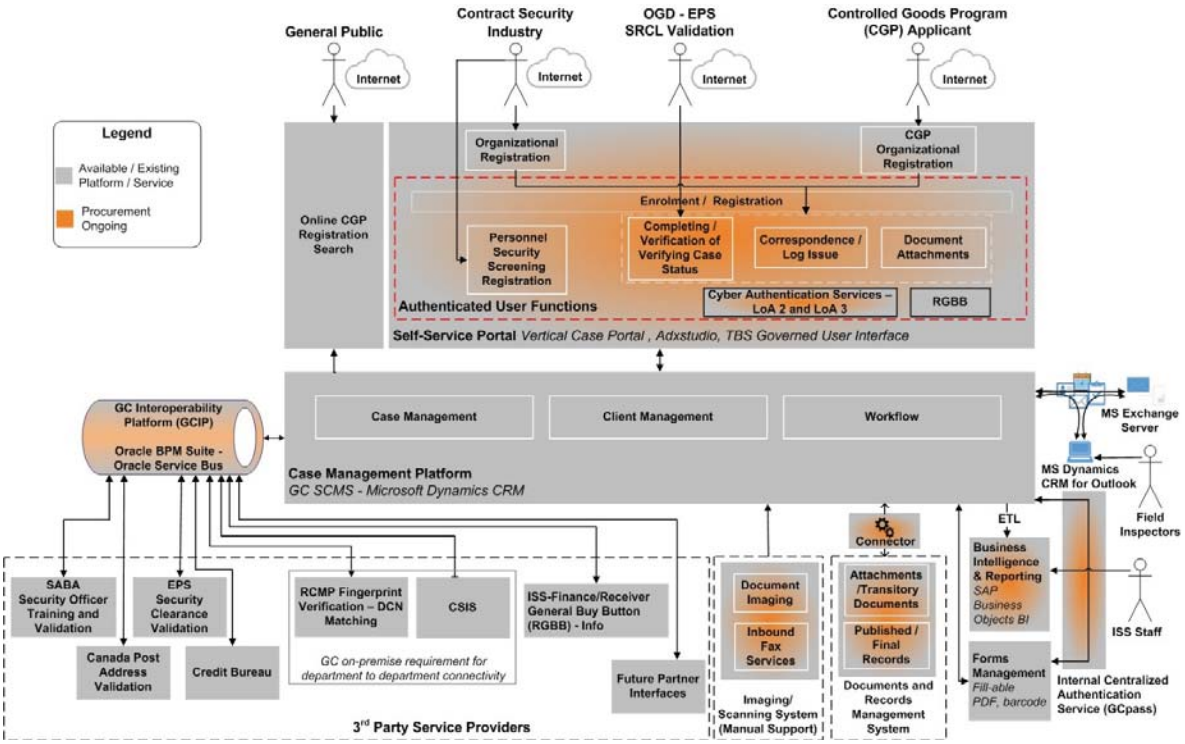


Figure 2: High level ISST Solution architecture diagram.

Microsoft Dynamics CRM is the core platform of the ISS Solution providing capabilities such as Case and Client Management as well as workflows for business process automation. Access to this platform will be required by ISS support staff after being authenticated via the GCpass authentication service. Field inspectors will also be able to interact with the MS Dynamics CRM core platform using the off-line access capabilities using MS Dynamics CRM for Outlook.

External Users, such as Contract Security and Controlled Goods Program applicants, will access the functionality required for their business processes via the internet Web Portal, based on the Adxstudio technology. These users will gain access to the Portal after being authenticated at the appropriate level of assurance required by the

application being accessed by using GCKey authentication factor and cyber authentication service. There will be **no** direct access to the MS Dynamics CRM core platform by External Users.

Users' access to various application functionalities will be enabled by role-based-access privileges and configurations of the underlying technology platforms based on the users' application profiles.

This architecture leverages Enterprise IT Target Suites that are driven by the Chief Information Officer Branches (CIOB) of both TBS and PWGSC in an attempt to rationalize and standardize the application footprint for GC applications. Wherever possible, the Contractor must meet the requirements of the current solicitation, including any new requirements driven by business process re-engineering, by leveraging GC/PWGSC Enterprise Architecture approved technologies, available within the GC and/or PWGSC IT supply chain. If not possible, any proposed alternate technologies must be approved by GC and a plan to migrate said alternate technologies within the GC and/or PWGSC technology footprint must be developed and provided as part of the Solution proposal. All Solution components within the scope of this project must integrate with IT components used by GC and meet the requirement of a unified Solution. Controlled access for External Users will be through an Internet-based user-centric portal interface.

The identified suites that the Contractor must adhere to include, but are not limited to:

(a) Adxstudio Portals (Adxstudio Portals and/or ASP.NET web forms)
Portal Technology - The portal must be developed based on Adxstudio Portals technology, host web enabled forms (ASP.Net web forms), requests for and the receipt of services. The portal will be used by External Users with defined roles and rights.

(b) Dynamics CRM (On premise) 2015 (or higher)
Case Management Technology - The portal will interface with a Customer Relationship Management tool, MS Dynamics CRM (on premise) 2015 (or higher), to initiate, interact with, manage and perform case management activities. The Case Management tool is a centrally managed service and will be used by Internal Users having defined roles and rights.

(c) Microsoft Exchange Server, Outlook Client
GC e-mail – This technology will be used to support off-line capability for internal users such as field inspectors.

(d) SAP Business Objects
Business Intelligence Reporting - SAP Business Objects is the enterprise suite for Business Analytics. However, for this solution, functionality including internal user dashboards will first leverage the reporting capabilities provided with the Dynamics CRM 2015 (or higher) tools to deliver the operational reporting functionality. Strategic reporting capabilities, if not available through Dynamics CRM 2015 (or higher) will be delivered through the standard suite SAP Business Objects connected to a PureData warehouse. Reporting functionality must be available to both Internal and External users

(e) Oracle Service Bus
Information Sharing Technology - GC Interoperability Platform (GCIP – based on Oracle Service Bus (technology). Information sharing between ISS and partner organizations must be automated and managed in accordance with GCIP capabilities and the underlying Oracle Service Bus service bus technology.

The Contractor must provide IM/IT technical expertise in the areas of application development particularly with C# and Java; configuration and integration; business process re-engineering; information integration; and application and data security.

All Solution hardware will be provided by GC and no additional installation of hardware is required (other than those related to the network connectivity). Any software tools to be used by the Contractor that are not available from within the GC packaged inventory, must first be approved by GC prior to commencing the PWGSC installation process. The Contractor must work closely with Shared Services Canada (SSC) to ensure hardware capabilities meet or exceed the demands of the overall Solution.

1.2 TECHNICAL REQUIREMENTS

The Contractor must deliver a Solution that adheres to, but is not limited to, the following requirements:

SOW NUM	Requirement
Tech.01	Enables and implements Web pages encoded in UTF-8.
Tech.02	Enables and implements 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.03	Provides functionality to allow External Users to export outputs such as reports and search results, including information in tabular and graphical format, in any format that specifically meets WCAG 2.0 requirements.
Tech.04	Adheres to best practices for securing web services, such as NIST SP 800-95 Guide on Secure Web Services and NIST SP 800-44 Version 2 Guidelines on Securing Public Web Servers.
Tech.05	Supports automatic termination of an open web session after a period of inactivity as determined by GC.
Tech.06	Provides functionality to allow Internal Users to export outputs such as reports and search results, including information in tabular and graphical format, in the following file formats provided that they comply with WCAG 2.0 techniques (http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/ws-nw/wet-boew-eng.asp) for testing conformance: (a) PDF (Adobe PDF); (b) DOC, DOCX (MS word 2013 and above); and (c) XLS, XLSX (MS Excel 2013 and above).
Tech.07	Supports the most recent GC Internet Browser standard (currently Microsoft Internet Explorer 11), and two previous major versions of the Microsoft browser as the standard evolves.
Tech.08	Compatible with major internet browsers supporting TLS 1.2 encryption currently available (including but not limited to Firefox, Safari and Chrome. See glossary (APPENDIX 5 to ANNEX A) for additional information).

SOW NUM	Requirement
Tech.09	Supports the capability to run as a secure web browser-based solution that does not require any other desktop software to be installed on the Internal User's workstation besides a web browser, "Microsoft Dynamics CRM for Outlook" providing offline Case Management capabilities and MS Outlook.
Tech.10	Supports the capability of accepting and uploading supporting documents and attachments with a maximum size possibly greater than 30 Mbytes, and of any file format.
Tech.11	Supports validation and confirmation of data entry by field type, data size, table properties and pre-configured list of values (e.g. only valid postal code format will be accepted for postal code).
Tech.12	Utilizes Adxstudio Portals, to create a web portal, aspx.net web forms to gather and exchange information from the web portal, is integrated with MS-Dynamics CRM 2015 (or later) entities and supports Tech.14 and Tech.18.
Tech.13	Provides an architecture style that enables robust error handling, recovery and notification to Users when online errors occur.
Tech.14	Incorporates best practice web application design principles for usability (i.e. to leverage W3 Web Application Best Practices including enabling/disabling buttons, options and flows based on User entered values, the reduction of needless prompting, etc.).
Tech.15	Utilizes to the maximum degree possible, the on-board reporting functionality of the MS Dynamics CRM 2015 (or later) application to; provide operational reporting and dashboard capability to the internal user community, and when possible, the strategic reporting capabilities.
Tech.16	Utilizes the capabilities of the GC Corporate Business Intelligence platform to deliver reporting functions not available from the Dynamics CRM 2015 (or later) based solution. This will require the contractor to create, Extract, Transform and Load (ETL) scripts which will automatically copy data from the solution database(s) to the GC Corporate Business Intelligence platform to provide reporting and dashboard capability. The Contractor will develop any report or dashboard required to support business decisions.
Tech.17	Meets at a minimum "Protected B, Medium Integrity, Medium Availability" (PB/M/M) security profile requirement.
Tech.18	Ensures conformance with the GC Web Standards and Web Accessibility requirements for the Self-Service Portal.
Tech.19	Supports scalability, should an expansion of the user community or Solution functionality be required to support GC initiatives.
Tech.20	Provides a response in the form of acknowledgement or case number to an external user within an acceptable response time (near real-time) after a single, properly completed request is submitted (the acceptable response time will be determined by GC).
Tech.21	Creates and sends information to Users via notifications.

SOW NUM	Requirement
Tech.22	Ensures support of the open architecture concept and allows (or permits) access to its services and functionalities through APIs, Web services, and similar technology.
Tech.23	Supports data exchanges to and from legacy systems during the transitional period using: (a) Near Real-Time or batch; (b) Web services / APIs; (c) XML and/or Flat file; (d) Export and import of data and content; and (e) Enterprise messaging/Service Bus.
Tech.24	Uses a Managed Secured File Transfer (MSFT) available service for file exchange.
Tech.25	Supports integration with smart PDF/ bar codes embedded forms accessed by hand held or other scanning tools to facilitate paper-based case processing.
Tech.26	Leverages GC and IT industry best practices and standards that have been adopted widely for building and maintaining a high-performing IT system to: (a) Provide easy-to-use Web applications; (b) Ensure and maximize the maintainability of the Solution; (c) Ensure and achieve high level reliability; (d) Ensure scalability and sustainability; and (e) Deliver acceptable system performance.
Tech.27	Supports GC's strategic plans for application interoperability, including, at a minimum by: (a) Exposing its functionality through an API that leverages industry-standard API protocols (functionality to be exposed includes the ability to invoke, if required, business processes within the Solution); and (b) Complying with GC standard - GC Interoperability Platform (GCIP) that will be standardized on Oracle Service Bus technology.
Tech.28	Interoperates with GC's IT stack (i.e. infrastructure and platform) without significant changes to the existing GC infrastructure or changes to desktops. The following is a list of types of expected technologies that must be supported: (a) SAML 2.0 (b) JSON (c) Kerberos (d) X.509 (e) LDAP (f) RBAC (g) OAuth (h) SOAP (i) REST (j) oData

SOW NUM	Requirement
Tech.29	Provides structured and modular external interfaces which allow information exchange between the Solution and other systems through a secure communications infrastructure. These interfaces include, at a minimum: (a) An intranet or extranet for the business processes described in "Section 2: Business Requirements"; (b) Web services – third party data feeds; (c) Commercially available third party security components such as Public Key Infrastructure (PKI) products; and (d) GC or NGO systems containing supporting information needed to process transactions.
Tech.30	Interoperates with other systems and platforms, as indicated in the diagram above, using as a minimum the following: (a) APIs; (b) Export and import of data and content; and (c) Simple Object Access Protocol (SOAP) based messages and/or file exchanges over (Oracle Enterprise Service Bus (ESB)).
Tech.31	Includes protection for transactional data, in transit and at rest through the usage of CSE, and TBS approved encryption algorithms and/or acceptable (to GC) alternatives.

The Contractor must:

SOW NUM	Requirement
Tech.32	Establish and support, for the duration of the contract, distinct staging environment(s) at the application level as necessary for the purpose of configuring, testing, deploying and training for the new Solution release. After solution release, some or all of the environments will persist and be used for ongoing activities, therefore the contractor must ensure a seamless transfer of configured environments to GC.
Tech.33	Design, develop, configure, test and support the Solution database to store, manage and protect data up to Protected B level.
Tech. 34	Develop Logical and Physical architecture blueprints, under the guidance of GC using the GC templates, and construct the Solution based on the Conceptual architecture.
Tech.35	Ensure the transfer of technical system knowledge to PWGSC staff and ensure that copies of all system documentation, including but not limited to: security, functional and non-functional configurations, build and run books are provided to PWGSC prior to completion of the Work.

SOW NUM	Requirement
Tech.36	Design and create a data architecture which: (a) Includes all appropriate data models, specifically, conceptual, logical, and physical; (b) Defines, in cooperation with PWGSC, policies, rules and any standards for data governance including how data is stored, arranged, integrated, and put to use within the solution; (c) Includes data dictionaries; (d) Will operate within the ISS solution environment; (e) Supports all ISS business processes; and (f) Supports the security requirements herein described (See Section 5 for IT Security Requirements).
Tech.37	Work with the GC to perform data gap analysis, and data mapping exercises between the legacy systems, and the solution.
Tech.38	Develop detailed interface documentation, including but not limited to: (a) Concept of Operations; (b) Systems Overview; (c) Interface Overview (for every Interface in, to and from the application); (d) Functional Allocation; (e) Data Transfer; (f) Transactions; (g) Security and Integrity; (h) Detailed Interface Requirements; (i) Interface Processing Time Requirements; (j) Message (or File) Requirements; (k) Communication Methods; (l) Security Requirements; (m) Qualifications Methods; (n) Approvals; and (o) Record of Changes.

SECTION 4: SECURE ACCESS

This section defines the Secure Access and User Authentication requirements for the Solution.

1.1 REQUIREMENTS OVERVIEW

The Contractor must provide secure access for two general groups of Users: Internal Users (e.g. Government employees) and External Users (e.g. Controlled Goods Program applicants (See APPENDIX 3 to ANNEX A)).

For the Internal User group, the secure access provided by the Contractor must interoperate with GC's Identity, Credential and Access Solution (GCpass (ICAS)) service, in particular, the Credential Management components of the Solution including:

(a) Managed user credentials;
(b) Authentication service for all information; and
(c) Support of Electronic Signatures by enabling and supporting Users to provide an electronic consent field in lieu of signature.

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 referred to as "myKEY". "myKEY" is currently in use at PWGSC (and is available GC wide), providing resources for authentication purposes of GC employees to GC systems requiring enhanced access controls. Treasury Board is leading the change to migrate from "myKEY" to GCpass to better serve the GC security needs.

For External User groups, the secure access provided by the Contractor must interoperate with:

(a) "GCKey" , an externally available, GC supported credential service; and
(b) "Secure-Key Concierge" (also known as Sign-In Partners), which is a partnership between major Canadian Banking institutions and Canada.

1.2 DETAILED REQUIREMENTS

1.2.1 Internal Users

The Contractor must deliver a Solution that adheres to, but is not limited to, the following requirements:

SOW NUM	Requirement
SecureInt.01	Integrates with myKEY authentication service provided by SSC.
SecureInt.02	Ensures User Authentication using myKey and a second authentication component (such as shared secrets) at logon to the Solution.
SecureInt.03	Complies with the Lightweight Directory Access Protocol (LDAP).
SecureInt.04	Links a myKey credential to a respective User account.

SOW NUM	Requirement
SecureInt.05	Limits, by user role, the number of allowable simultaneous logons into the Solution for the same unique User account in accordance with the security standard.
SecureInt.05	Ensures that SCMS is accessible through a VPN.

1.2.2 External Users

The Contractor must deliver a Solution that adheres to, but is not limited to, the following requirements:

SOW NUM	Requirement
SecureExt.01	Integrates with GC's GCKey and Secure-Key Concierge.
SecureExt.02	Ensures User Authentication using GCKey or Secure-Key Concierge and a second authentication component (such as shared secrets) at logon to the Solution's Web Portal.
SecureExt.03	Links a GCKey or Secure-Key Concierge credential to a respective User profile.
SecureExt.04	Limits, by user role, the number of allowable simultaneous logons into the Solution for the same unique User account, in accordance with the security standard.
SecureExt.05	Complies with TBS Cyber Authentication and LoA2 and LoA3 level authentication tokens where applicable as per guidance provided by CSE in its publication "ITSP.30.031 v2 User Authentication Guidance For Information Technology Systems".

SECTION 5: IT SECURITY REQUIREMENTS

This section defines the security requirements for the Solution.

1.1 REQUIREMENT OVERVIEW

1.1.1 Security Assessment and Authorization Process

The GC has invested significantly in IT systems, and desires to protect to the highest degree possible, the assets of its business. To accomplish this, a strong Security Assessment and Authorization (SA&A) process has been instituted. All information systems must pass a number of assessment gates during development in order to be released into the production environment. High level requirements associated with various SA&A Gates are summarized in the table below while detailed requirements are defined in the Detailed Requirements sub-section.

SA&A Gate	Requirement
SAAG.01	The Contractor must complete: (a) Security High Level Solution Design (SHLSD); and (b) Security Requirements Traceability Matrix (SRTM).
SAAG.02	Following acceptance of the Work for SA&A Gate 1, and subject to approval by the Project Authority, the Contractor must completed: (a) Security Detailed Solution Design (SDSD); (b) Updated Security Requirements Traceability Matrix (SRTM); (c) Change Management Procedures; (d) Operational Security Procedures; and (e) Security Installation Procedures.
SAAG.03	Following acceptance of the Work for SA&A Gate 2, and subject to approval by the Project Authority, the Contractor must complete: (a) Security Installation Verification Plan; (b) Security Installation Verification Report; (c) Security Integration Test Plan; (d) Security Integration Test Report; (e) Updated SRTM with Security Integration Test Report mapping to security requirements; (f) Vulnerability Assessment Plan; and (g) Updated SRTM with Vulnerability Assessment Report mapping to security requirements.

1.1.2 Security Control Catalogue

The following provides a very high level description of the Information Technology Security Guidance 33 (ITSG-33) security control catalogue which is organized into classes and control families. These control families apply to the ISS security requirements and are further addressed by the Detailed Requirements defined in this ANNEX. The controls satisfying the full Solution are embedded in the existing technical implementations, such as the SCMS.

Since the full Solution will be primarily an integration exercise, the full suite of Solution controls will be assessed throughout the development of the Solution using the Security Assessment and Authorization process. These control families are the basis of securing the Solution and its Data.

1.1.2.1 Technical Security Class

The Technical Security Class consists of the following control families:

(a) Access control: security controls that support the ability to permit or deny user access to resources within the information system;
(b) 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;
(c) 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
(d) 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.

1.1.2.2 Operational Security Class

The Operational Security Class consists of the following control families:

(a) Awareness and training: security controls that deal with the education of users with respect to the security of the information system;
(b) Configuration management: security controls that support the management and control of all components of the information system (e.g., hardware, software, and configuration items);
(c) Contingency planning: security controls that support the availability of the information system services in the event of component failure or disaster;
(d) Incident response: security controls that support the detection, response, and reporting of security incidents within the information system;
(e) Maintenance: security controls that support the maintenance of the information system to ensure its ongoing availability;
(f) Media protection: security controls that support the protection of information system media (e.g., disks and tapes) throughout their life cycle;
(g) 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;
(h) 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
(i) System and information integrity: security controls that support the protection of the integrity of the information system components and the data that it processes.

1.1.2.3 Management Security Class

The Management Security Class consists of the following control families:

(a) Security assessment and authorization: security controls that deal with the security assessment and authorization of the information system;
(b) Planning: security controls that deal with security planning activities including privacy impact assessments;
(c) Risk assessment: security controls that deal with the conduct of risk assessments and vulnerability scanning; and

(d) System and services acquisition: security controls that deal with the contracting of products and services required to support the implementation and operation of the information system.

1.2 DETAILED REQUIREMENTS

The requirements in the table below were developed from the Protected B/Medium Integrity/Medium Availability (PB/M/M) profile from ITSG-33. Many of the ITSG-33 controls overlap or reference one another. The requirements listed here allow good coverage of the PB/M/M requirements, and excludes those items that are expected to be covered by PWGSC as an organization through existing technology implementations rather than ISS or this Solution specifically. The final version of the Security Requirements Traceability Matrix will list the controls required to support the ISS Solution. The requirements below are not exhaustive and may evolve during the Contract Period.

The Contractor must deliver a Solution that meets the following IT security requirements, but is not limited to:

Category	SOW NUM	Requirement
Access Control and Account Management	SC.01	The Solution must: (a) Enforce role-based access controls for all individual users; (b) Organize users into roles designed using the principles of “least privilege” and “need-to-know”; (c) Automatically disable inactive or unused accounts after a period of time determined by the business; (d) Create audit records regarding the creation, modification, removal, enabling, and disabling of accounts; (e) Log users out, or lock sessions and conceal any information being displayed, after an appropriate period of inactivity in accordance with GC policies and industry best practices; (f) Retain the session lock until the user re-establishes access using established identification and authentication procedures; (g) Attribute the creation of any account to a single, specific individual; (h) Require the use of non-privileged accounts or roles, when accessing non-security functions; (i) Limit the number of unsuccessful login attempts before locking the account; (j) Notify the user of the last successful login, including date and time, and the number of unsuccessful login attempts since the last successful login; (k) Notify the user of any changes to their account roles and permissions since the last successful login; (l) Provide the functionality to set, define, change and display security attributes of information in storage, in process and/or in transmission by authorized individuals; and (m) Provide the functionality to display a logon banner.
	SC.02	The Contractor must document the roles and the responsibilities, features, and capabilities of contractors, employees, and third-party users as they relate to PWGSC ISS Solution information assets and security.
	SC.03	The Contractor must implement separation of duties for Users, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the User.

Category	SOW NUM	Requirement
Audit and Accountability	SC.04	The Solution must: (a) Generate audit records in a standardized format containing, at a minimum, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event; (b) Provide the functionality to set warnings and alerts for different audit conditions (i.e. audit record reaches maximum storage capacity and other audit failures); (c) Generate audit records of security events in a format suitable for submission to a Security Information and Event Management (SIEM) system; and (d) Timestamp audit records using an accurate time source.
	SC.05	The Contractor must document the content and format of the security audit records, providing appropriate estimates of the expected storage requirements and bandwidth requirements to manage the audit records. The documentation must also be clear with respect to the priority or importance of audit records so that alerting and monitoring rules can be derived.
	SC.06	The Solution must: (a) Protect audit information from unauthorized access, modification, and deletion; and (b) Backup audit records onto a different system or media than the system being audited on a schedule as specified by PWGSC.
Identification and Authentication	SC.07	The Solution must: (a) uniquely identify and authenticate organizational users; and (b) Have authentication mechanisms that meet Communications Security Establishment (CSE) requirements and guidelines, Treasury Board of Canada Secretariat (TBS) policies, and best practices.
	SC.08	The Solution must: (a) Allow mutual authentication of connections, between the Solution and other domains as specified by PWGSC, and exclusively exchanges information with these other domains using mutual authentication; (b) Ensure that the integrity and confidentiality of data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by PWGSC; and (c) Conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 and (ITSG) ITSG-38.

Category	SOW NUM	Requirement
Information System Connections	SC.09	The Contractor must: (a) Fully document any connections between IT systems including data descriptions, data flows, security and access requirements and mechanisms, performance, and reliability expectations; and (b) Provide evidence that providers of external information system services comply with organizational information security control requirements and employ security controls in accordance with the TBS Security and Contracting Management Standard.
Configuration Management	SC.10	The Contractor must fully document the baseline configuration of the Solution as it pertains to the requirements.
	SC.11	The Contractor must conduct and assess the security impact of changes for new software implementations, major configuration changes and patch management by: (a) Analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; (b) Informing PWGSC of potential security impacts prior to change implementation, and (c) Checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements.
	SC.12	The Contractor must only allow authorized software, as documented by the Contractor and approved by PWGSC, to execute on the Solution.
	SC.13	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 (PWGSC CIOB).
	SC.14	The Contractor must follow the PWGSC Change Request Management process for any changes to the Solution.
Contingency Planning	SC.15	The Contractor must fully document the contingency plan for the continued operation of ISS business lines to meet the minimal contingency planning requirements for the PB/M/M at a minimum profile of ITSG-33.

Category	SOW NUM	Requirement
Information Security Architecture	SC.16	The Contractor must document the information security architecture for the Solution that: (a) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of information; (b) Describes how the information security architecture is integrated into and supports the enterprise architecture; and (c) Describes any information security assumptions about and dependencies on, external services.
	SC.17	The Contractor must provide a Security High Level Solution Design (SHLSD) that includes, at a minimum: (a) A high-level component diagram that clearly shows the allocation of services and components to network security zones and identifies key security related data flows; (b) The architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer); (c) A description of the network zone perimeter defences; (d) A description of the use of virtualization technologies, where applicable; (e) Descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers; (f) Descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements; (g) A description of the approach for: i. Remote management; ii. Access control; iii. Security management and audit; iv. Configuration management; and v. Patch management. (h) Justification for key design decisions.
	SC.18	The Contractor must provide a Security Detailed Service Design (SDSD) that includes, at a minimum: (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.

Category	SOW NUM	Requirement
Boundary Protection	SC.19	The Solution must: (a) Be implemented in such a way as to be resistant to denial of service attacks in order to meet ISS availability targets; (b) Monitor and control communications at external boundaries of the Solution (internet facing and GC facing); (c) Be configured to deny communication by default and allows only authorized communications; (d) Be able to detect and deny communications that appear to pose a threat to internal or external systems, and attribute such communications to an individual to the greatest extent practical; (e) Protect the authenticity of communications sessions; (f) Invalidate session identifiers upon logout or other session termination; and (g) Use unique session identifiers and only recognize system-generated session identifiers.
	SC.20	The Solution must fail securely in the event of an operational failure of a boundary protection device.
Protection of Information	SC.21	The Solution must: (a) Protect information in transit between systems; (b) Protect information at rest in the system; and (c) Provide the functionality to integrate cryptographic solutions in accordance with CSE recommendations and TBS policies.
Mobile and Malicious Code	SC.22	The Solution must: (a) Employ malicious code protection mechanisms at entry and exit points to the Solution that can detect and eradicate malicious code; (b) Maintain the malicious code protection mechanisms in an up-to-date state in accordance with organizational configuration management policies; and (c) Use mobile code only in ways that are fully documented and maintain the other security protections in the solution.
Information System Monitoring	SC.23	The Solution must: (a) Be able to detect attacks, indicators of potential attacks and unauthorized local, network, and remote connections; and (b) Notify security administrators of such detections.
Security Attributes	SC.24	The Solution must provide privileged users the capability to define or change the value of security attributes on objects.
Least Functionality	SC.25	The Solution must be configured in accordance with industry best practices and GC policies for information system hardening; including, but not limited to disabling unnecessary ports, protocols and services.

Category	SOW NUM	Requirement
	SC.26	The Contractor must document all ports and protocols required by the Solution. The documentation must include, at a minimum: (a) The port, protocol, or service being used; (b) A description of the information being transferred in that port/protocol/service; (c) A description of the flow (source and destination); and (d) Any firewall or routing rules necessary to support the communication.
Security Testing	SC.27	The Contractor must: (a) Create and implement a security assessment plan; (b) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; (c) Implement a verifiable flaw remediation process; and (d) Correct flaws identified during security testing/evaluation. Prior to being authorized for use in a production environment, the solution must be scanned for vulnerabilities using industry standard tools, and those vulnerabilities found must be addressed to the satisfaction of PWGSC.
Information System Recovery and Reconstitution	SC.28	The Contractor must fully document the procedures to recover or reconstitute the Solution in accordance with the minimal requirements of PB/M/M profile from ITSG-33.
Unsupported System Components	SC.29	The Contractor must document a plan for the maintenance and support of the Solution components and sub-components such that the Solution will not be left in a partially supported state due to lack of sub-component support, nor with unpatched vulnerabilities due to sub-components.
Cryptographic Key Establishment and Management	SC.30	The Solution must establish and manage cryptographic keys in accordance with guidelines promulgated by CSE.
Information Input Validation	SC.31	The Solution must check the validity of input information.
Incident Management	SC.32	The Contractor must assist the GC and aid in the response to all suspected or actual incidents related to the Solution for the duration of the contract.
	SC.33	The Contractor must report all suspected or actual privacy and security violations as Security Incidents for the duration of the contract.

Category	SOW NUM	Requirement
	SC.34	The Contractor must provide support and assistance to the GC in implementing mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, and removing malicious malwares) to contain a Security Incident and to protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level for the duration of the contract.
	SC.35	The Contractor must provide support and assistance to the GC in the development of an incident response plan.
	SC.36	The Contractor must provide support and assistance to the GC in the development of a Security Incident post-mortem report when required by PWGSC for the duration of the contract.
	SC.37	The Contractor must for the duration of the contract create one or more incident tickets for each incident detected.
Continuous Monitoring	SC.38	The Contractor must for the duration of the contract assist and support the GC in ensuring that the security posture of the Solution is maintained by continuously identifying and notifying the GC of: (a) Threats and vulnerabilities; and (b) Malicious activities and unauthorized access.
Risk assessment	SC.39	The Contractor must develop a Solution vulnerability mitigation plan approved by PWGSC within five (5) Business Days of completion of a vulnerability assessment that includes proposed protection measures to mitigate the risks identified from the vulnerability assessment.
	SC.40	The Contractor must for the duration of the contract implement patches and corrective measures as part of vulnerability assessment activity. 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.
Security (General)	SC.41	The Solution, at a minimum, must comply with the requirements of the PB/M/M profile in ITSG-33, ANNEX 4A (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-ann4a-1-eng_4.pdf).
	SC.42	The Contractor must provide a Security Integration Test Plan as part of the IT Security Plan submission to GC for approval that must include at a minimum: (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).

Category	SOW NUM	Requirement
	SC.43	The Solution must maintain data integrity during conversion between various protocols and data formats.
	SC.44	The Solution must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.
General	SC.45	The Contractor must obtain PWGSC's approval for the use of external (i.e., non-Contractor) information systems for the delivery of the Solution.
	SC.46	The Contractor must obtain PWGSC's approval before making any Solution content publicly available.
	SC.47	The Contractor must provide Operational Security Procedures to GC that includes, at a minimum: (a) For each Privileged User role: i. Schedule of security-relevant actions to be performed in order to maintain the security posture of the ISS; 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.
	SC.48	The Contractor must provide detailed Security Installation Procedures to GC that includes, at a minimum: (a) Steps necessary for the secure installation and configuration; (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).

Category	SOW NUM	Requirement
	SC.49	The Contractor must provide a Security Installation Verification Plan and Verification Report to GC that includes, at a minimum: (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; iii. Expected results (i.e., pass/fail criteria); iv. Actual results; and v. A description of deviation and how each was resolved.
	SC.50	The Contractor must for the duration of the contract provide support and assistance to GC in conducting the security installation verification in accordance with the approved Security Installation Verification Plan.
	SC.51	The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.
	SC.52	The Contractor must conduct security integration testing in accordance with the Security Integration Test Plan.
	SC.53	The Contractor must provide the Security Integration Test Report that includes, at a minimum, for each of the test items in the 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.
	SC.54	The Contractor must use non-sensitive information or data masking techniques to replace sensitive information in any non-production environment.

Category	SOW NUM	Requirement
	SC.55	The Contractor must update throughout the SA&A process a SRTM to GC that includes, at a minimum: (a) The security requirement identifier; (b) An identifier that maps the security requirement to the corresponding statement in the ANNEX A (e.g., heading or line identifier); (c) The security requirement statement; (d) A description of how the security requirement is addressed in the SHLSD and SDLD 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., solution continuity plan); (f) Tracing (a reference to an identifiable element) to the SHLSD and SDLD to allow the GC to confirm that the security safeguards satisfy the security requirements; (g) 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; and (h) 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.
Account Management	SC.56	The Solution must create user accounts based on GC-approved account roles.
Account Management &Least Privilege	SC.57	The Solution must audit user account activities and account privileges, and create report based on selectable criteria.
Information Flow Enforcement	SC.58	The Solution must only accept the transmission of GC-approved file data types.
	SC.59	The Solution and solution platform must analyze inbound and outbound information in order to detect malicious codes and unacceptable content.
Concurrent Session Control	SC.60	The Solution must limit the number of concurrent sessions for privileged account, non-privileged accounts and any other types of accounts as specified by the GC.
Session Termination	SC.61	The Solution must automatically terminate a user session after a period of user inactivity as specified by the GC.
	SC.62	The Solution must: (a) Logout user-initiated communications sessions whenever authentication is used; and (b) Display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.
Security	SC.63	The Solution must have mechanisms to maintain the association and integrity of GC-defined security attributes.

Category	SOW NUM	Requirement
Attributes	SC.64	The Solution must implement proper technologies/techniques with the level of assurance defined by the GC in associating security attributes to information.
Data Mining Protection	SC.65	The Solution must employ data mining prevention and detection techniques such as (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) notifying organizational personnel when atypical database queries or accesses occur for data storage objects such as databases, database records, and database fields to adequately detect and protect against data mining.
Protection of Audit Information	SC.66	The Solution must implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
Non-Repudiation	SC.67	The Solution must support the ability to protect against an individual (or process acting on behalf of an individual) falsely denying having sending or receiving a transaction.
	SC.68	The Solution must (a) Bind the identity of the information producer with the information to the GC defined strength of binding and; (b) Provide the means for authorized individuals to determine the identity of the producer of the information.
	SC.69	The Solution must (a) Validate the binding of the information producer identity to the information at the frequency defined by the GC; and (b) Perform GC defined actions in the event of a validation error.
Identification and Authentication (organizational users)	SC.70	The Solution must implement multifactor authentication for network access to (a) Privileged accounts; and (b) Non-privileged accounts.
Authenticator Management	SC.71	The Solution must dynamically provision identities.
Re-Authentication	SC.72	The Solution must re-authenticate users and devices when authenticators change; when roles change; when security categories of information systems change; when the execution of privileged functions occurs; after a fixed period of time; periodically or other situations defined by GC.
Software, Firmware and Information Integrity	SC.73	The Solution must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to software, firmware, and to information.

Category	SOW NUM	Requirement
Information Output Filtering	SC.74	The Solution must validate information output from the various ISS components to ensure that the information is consistent with the expected content.

SECTION 6: TESTING MANGEMENT

This section defines the testing requirements for the Solution.

1.1 REQUIREMENT OVERVIEW

As a guiding principle, the Contractor must conduct all required testing in a comprehensive, thorough, open ended, recursive and timely manner. The Contractor must ensure any methodology used, contains quality processes throughout the design, configuration and testing phases. Quality processes will:

(a) Ensure earlier and better test plans;
(b) Permit testers to have time to understand the solution;
(c) Ensure testing is done correctly the first time;
(d) Validate each step and component before moving to the next one; and
(e) Quality of the specifications and design increase through feedback generated by the scrutiny of test planning and design.

The Contractor must initially develop, and maintain the Solution Test Plan through all phases of development, updating the document as business processes emerge in order to create appropriate test scripts. It is expected that the Contractor will utilize testing techniques including but not limited to; (functional analysis, equivalence, path analysis, boundary value, user scenario, checklists and risk analysis) to conduct testing within the: Unit, System, Functional, End to End, Security (Vulnerability Assessment to be conducted by SSC/PWGSC), and Client Acceptance, cycles of testing. The Contractor must outline in detail the test processes to be used within the Test Plan.

The Contractor will be provided suitable development environments in which to configure the approved business processes prior to testing.

The Contractor must manage and perform the testing related work throughout the Contract Period that includes, but is not limited to, the following activities:

(a) Develop a Baseline Test Plan which is updated as the solution design advances;
(b) Create a Defect Management Framework that must include:
    i. The usage of a defect tracking tool which informs the project team of issues, impacts and resolution;
    ii. Scale of severity for encountered defects;
    iii. Test team meetings to discuss related items as required by the Project Authority; and
    iv. Standing meetings between Contractor and Project Authority.
(c) Testing documentation, including:
    i. Test Entry and Exit criteria;
    ii. Test cases and test scripts; and
    iii. Acceptance criteria;
(d) Updating the Project Authority of any possible setbacks or issues that have been encountered during testing.

1.2 DETAILED REQUIREMENTS

The Contractor must meet the following testing requirements, but is not limited to:

Category	SOW NUM	Requirement
Test Management (General)	TM.01	Before commencement of the development Work, the Contractor must develop the Testing Strategy and Plan. Subject to the approval of the Project Authority, the Plan must include, as a minimum, the following information for all stages of the required testing: (a) A high-level of overview of the proposed testing strategy; (b) A Defect Management Framework; (c) Entry and exit strategy; (d) Meetings between the Contractor and Project Authority; and (e) On-going risk management and mitigation strategy.
	TM.02	For each testing phase, the Contractor must develop testing Scripts pertinent to the testing technique used.
	TM.03	The Contractor must develop and maintain the Defect Tracking Report throughout all testing stages. The Report must, as a minimum, include the following information: (a) An ongoing log of all defects found during testing of the solution; and (b) Descriptions of defect, level of severity, stage of testing discovered, actions taken to resolve, and current status. The Contractor must provide the Report to the Project Authority as and when requested.
	TM.04	The Contractor must develop and maintain the Weekly (testing) Status Report throughout all testing stages. The Report must, as a minimum, include the following information: (a) A summary of actions performed in the past week as well as next steps in the testing stage; and (b) The most recent copy of defect tracking report. The Contractor must provide the Report to the Project Authority at the beginning of each week of testing.
	TM.05	Upon completion of end-user testing, the Contractor must provide the Project Authority the Test Closure Report that includes the final copy of the Defect Tracking Report, along with tester signed off test cases and all other relevant testing documentation and metrics. The Report is subject to the acceptance and approval of the Project Authority.
	TM.06	Upon completion of testing and prior to any release to production, the Contractor must provide the Project Authority the Functional Specifications that document all functional specifications created and tested for in the Solution.
	TM.07	The Contractor must provide a series of regression testing scripts that can be used by the ISS to facilitate the testing of solution base functionalities within future releases to the

Category	SOW NUM	Requirement
		solution.
	TM.08	The Contractor must provide a presentation of options for Project Authority approval for encountered defects that have a significant impact to the Solution's design, timeline, etc. or as required by the Project Authority.
Test Management (Test Type)	TM.09	The Contractor must: (a) Conduct Unit Testing, Path Analysis, System, Integration and Functional Testing on each module or component of the Solution; (b) Create and provide Test Scripts; (c) Log and resolve all defects found before performing the next-stage testing; and (d) Ensure testing cycles continue until a full cycle is completed without any new bugs or defects. The completion of testing is subject to the final approval of the Project Authority.
	TM.10	The Contractor must: (a) Coordinate User Acceptance (UAT) Testing upon completion of Functional Testing (Regression, End-to-End and Scenario testing is considered a part of UAT Testing); (b) Develop and provide Testing Scripts (including Regression testing); (c) Ensure that the testers have the ability to log defects, bugs and anomalies whether part of a documented test case or not; (d) Ensure testing cycles continue until a full cycle is completed without any bugs or defect; and. (e) The Contractor must log and address all testing defects before final-sign off can be obtained from the Project Authority.
	TM.11	The Contractor must conduct Data Validation Testing to validate and ensure the accuracy of the data received from the legacy systems into the new Solution. The completion of Data Validation Testing is subject to the final approval of the Project Authority.
	TM.12	The Contractor must conduct Performance and Load testing of the Solution.

SECTION 7: MANGEMENT AND OVERSIGHT

This section defines the requirements of the project and organizational change management for the Solution.

1.1 PROJECT GOVERNANCE

The Contractor is responsible for the design, development and implementation of the Solution that includes business transformation services. The Contractor is responsible for, but not limited to:

(a) Project management and planning services;
(b) Change Management services including training and communications;
(c) Business process reengineering services;
(d) Solution architecture and design services (including security requirements);
(e) Solution Development and Implementation services including security; and
(f) Data migration services.

At a high level PWGSC is responsible for:

(a) Overall project sponsorship and project management oversight;
(b) Review of deliverables and the provision of feedback and approvals in a timely manner;
(c) Provision of information and advice to the Contractor concerning functional and non-functional requirements;
(d) Coordinating, on behalf of the Contractor access to subject matter experts concerning functional and non-functional requirements;
(e) Coordinating, on behalf of the Contractor, meetings required to seek approval of project deliverables where stakeholders outside the ISST Project must be engaged (e.g. Enterprise Architecture approval of solution architecture);
(f) Securing all GC gating approvals; and
(g) Contract Management.

The ISST Project Organization is comprised of a number of sub-organizations, each with a different role.

(a) **PWGSC Industrial Security Sector (Project Authority)**
The ISS Project Authority acts on behalf of the business line. The ISS Project Authority has overall accountability and approval for the ISST Project and is responsible for, but not limited to:
   i. Decisions that have business and/or project impacts;
   ii. Reviewing and approving all business and overall project deliverables, e.g. training deliverables, communication deliverables, business process maps, strategies, plans, etc.;
   iii. Identification and coordination of business expertise required to support project activities such as, but not limited to testers, business analysts, etc.; and
   iv. Supporting the Contractor with business process reengineering work effort, data migration, change management, developing strategies and plans that will address the requirement to transition the organization from its current 'as-is' state to the 'to-be' state.

(b) **PWGSC Chief Information Officer (CIO) Branch**
The PWGSC Chief Information Officer (CIO) Branch represents the technical arm of the project, both from a PWGSC perspective and a Shared Services Canada (SSC) perspective. CIO Branch is responsible for providing IT coordination services and technical support services to the project and is responsible for, but not limited to:

i. Representing the PWGSC CIO Branch interests in the ISST Project in areas such as Solution Architecture, System security, web standards compliance, maintainability of the Solution, etc.;
ii. For reviewing and approving technical (IT) deliverables such as architectures, design specifications, etc.; and
iii. Ensuring that the various entities within the PWGSC CIO organization who are stakeholders in the ISST solution (IT Enterprise Architecture, IT Infrastructure, IT Security, Application and Database Support, etc.) are engaged in the project as necessary.

(c) **Shared Services Canada**
The Solution will be delivered by the Contractor using the SSC provided infrastructure such as servers, networks, databases, etc. Working with the Contractor, SSC will be responsible for, but not limited to:

i. Designing and implementing infrastructure that supports and enables the Solution;
ii. Reviewing and ensuring that security is addressed from an infrastructure perspective for the Solution;
iii. Participating in performance and load testing and sizing of the infrastructure as needed; and
iv. Participating in the security assessment and authorization process from an infrastructure perspective.

1.2 REQUIREMENT OVERVIEW - PROJECT MANGEMENT

The Contractor must deliver the Solution as outlined in this Statement of Work in collaboration with PWGSC. PWGSC will facilitate and coordinate access to the work environment. The Contractor is responsible for all project management services as well as overseeing the quality of work delivered by its Professional Services resources. The Contractor must perform all project management services necessary to plan, manage and deliver all the Work under the Contract as specified herein. The provision of these services must commence at Contract Award and is subject to review, approval and acceptance by the Project Authority.

1.3 DETAILED REQUIREMENTS - PROJECT MANGEMENT

The Contractor must meet the following project management requirements, but is not limited to:

Category	SOW NUM	Requirement
General	PM.01	The Contractor must ensure that all work is integrated with PWGSC activities, such that the scope, performance, time, quality, risk and issue elements associated with the Contract are fully managed, controlled and scheduled.
	PM.02	In alignment with industry best practices and the departmental National Project Management System (NPMS) policy, the Contractor must use a formal project management methodology to ensure that the work to be performed throughout the duration of the Contract conforms to the requirements of this ANNEX, its attachments and referenced documents.
	PM.03	The Contractor must deliver all softcopy documentation to the Project Authority in the

Category	SOW NUM	Requirement
		following formats: (a) Text documents or presentations using Microsoft Office (Word, PowerPoint, Excel), version 2013 or later; (b) Diagrams and flowcharts: Microsoft Visio, version 2013 or later; and (c) Project plans and schedules: Microsoft Project, version 2013 or later. The Contractor may request approval from the Project Authority to submit documents in other softcopy formats; this must be expressly authorized by the Project Authority. Approval is at Canada's sole discretion.
Project Management Team	PM.04	The Contractor must establish a Project Management Team. The composition of the Project Management Team is at the discretion of the Contractor however the Team must meet the following minimum requirements: (a) Led by a dedicated Senior Delivery/Project Manager who is responsible for the management and oversight of Solution integration and configuration described in this Contract. He/she must be dedicated on a full-time basis to the ISST Project, on-site at PWGSC in the National Capital Region (NCR). The Senior Delivery/Project Manager will be the Contractor resource for communicating the project status, risks, issues, project slippages and remediation and will be the liaison between PWGSC and the Contractor; (b) Prepare and maintain a document outlining the Contractor Organizational Model. Each of the Project Management Team members and their relationships must be named in the Contractor Organizational Model; (c) Prepare and maintain a document outlining the governance model, including a roles and responsibility matrix including the Contractor and GC entities for the project; and (d) Contractor Project Management Team must be located on site for the duration of the contract to facilitate planning, design, development, testing, training and deployment activities.
Professional Services Resources	PM.05	Throughout the entire Contract Period, the Contractor must provide and maintain qualified Professional Service (PS) resources who are able to produce, implement and execute the deliverables as outlined in ANNEX A.
Project Plan	PM.06	The Contractor must develop and maintain a Project Management Plan in accordance with industry best practices or standards and is subject to the approval of the Project Authority.
Project Schedule	PM.07	The Contractor must: (a) In collaboration with the Project Authority and based upon the ANNEX A, create, maintain and monitor the detailed Project Schedule including dependencies and OPI; (b) Implement, maintain and use an approved Project Schedule for the duration of the Contract. Changes affecting the Project Schedule can only be made through an approved Change Request; and (c) Identified changes to the Project Schedule as a result of Change Requests are to be incorporated into the project Risk Register. (d) Update the Project Schedule as the required during the project's progression or

Category	SOW NUM	Requirement
		when requested by the Project Authority.
Project Monitoring	PM.08	The Contractor, in collaboration with Project Authority, must create and maintain the Project Action Item Register that provides a list of all action items, identifies which are outstanding and completed; and at a minimum, is updated on a weekly basis and/or as required. The Contractor is not asked to provide the deliverable in the exact format presented below, but must provide all the following information: (a) Number of the action item; (b) Description of the action item; (c) Person responsible for following through (OPI); (d) Date Initiated; (e) Date due; (f) Status; (g) Percentage of Completion vs Baseline schedule; and (h) Comments.
	PM.09	The Contractor, in collaboration with Project Authority, must create and maintain the Project Meeting Agenda(s) as required. The Agendas must be circulated to the attendees' a minimum of one day before meetings. The Contractor is not asked to provide the deliverable in the exact format presented below, but must provide all the following information: (a) Subject; (b) Date of meeting; (c) Time of meeting; (d) Place of meeting; (e) Required attendees; (f) Optional attendees; (g) Action Items listed to be reviewed /discussed; and (h) Attachments as appropriate.
	PM.10	The Contractor, in collaboration with Project Authority, must create and maintain the Project Meeting Minutes as required. The Minutes must be circulated to attendees within two business days after the meeting. The Contractor is not asked to provide the deliverable in the exact format presented below, but must provide all the following information: (a) Meeting Title; (b) Date and time of meeting; (c) Attendees and absentees; (d) Minutes taken by; (e) Copy of minutes sent to; (f) Minutes of discussions; (g) Record of decisions taken; (h) Action items raised; (i) Other business; and (j) Next meeting information.
	PM.11	The Contractor, in collaboration with Project Authority, must create and maintain the Project Status Reports. The Project Status Reports must be presented and distributed on

Category	SOW NUM	Requirement
		a weekly or as required basis and include the following information, at a minimum: (a) Milestone Status; (b) Status and issues information relating to completion dates; (c) Identify any new risks to deliverables and outline mitigation strategies for risks already identified; and (d) Any requests for change.
	PM.12	The Contractor must provide Change Request Management Procedures to GC that includes, at a minimum: (a) Contractor resource roles and responsibilities for change request management; (b) How the Contractor will use the change request management process to support the development of the Solution; (c) Method used to uniquely identify configuration items; (d) Configuration item identification method; (e) Description of the change request management process, including the change review and approval process; (f) Means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items; (g) Measures used to enforce only authorized changes; (h) Procedures that the Contractor will use to accept modified or newly created configuration items; and (i) A Change Request Management log.
	PM.13	The Contractor must ensure that key Project Team members attend all project milestone events and project reviews including any other meetings between the Project Authority and the Contractor as required or requested by the Project Authority.
	PM.14	The Contractor, in collaboration with Project Authority, must create and maintain the Project Risk Register throughout the lifecycle of the project. Updates to the Project Risk Register must be provided as required or requested by the Project Authority. At a minimum the Project Risk Register must include: (a) Id #; (b) Description; (c) Response/Mitigation Strategy; and (d) Risk Likelihood & Impact.
	PM.15	The Contractor, in collaboration with Project Authority, must create and maintain the Project Issue Log throughout the lifecycle of the project. Updates to the Project Issue Log must be provided as required or requested by the Project Authority. At a minimum the Project Issue Log must include: (a) Id #; (b) Description; (c) Response/Mitigation Strategy; and (d) Risk Likelihood & Impact.
Project Implementation	PM.16	The Contractor must provide a proposed Solution Delivery Plan that appropriately addresses requisite activities and deliverables, respects the overall timeline of the

Category	SOW NUM	Requirement
		project, anticipated phased rollout approach and recursive communication, testing and training cycles. Identified deliverables within the Solution Deliver Plan should be reflected in the Project Schedule and Change Management activities. The Solution Delivery Plan should also align with the Key Activities outlined in APPENDIX 2 To ANNEX A.
Project Close-Out	PM.17	The Contractor must prepare and provide a Project Close-Out Report assessing that includes, but is not limited to: (a) Assessment of project performance; (b) Identification of lessons learned; (c) Confirmation that essential contractual and other project closure activities have been completed; (d) Outstanding Issues; (e) Transfer of assets, deliverables and ongoing administrative functions; and (f) Measurement of post implementation benefits/outcomes (KPI) delivered by the project.

2.1 REQUIREMENT OVERVIEW - CHANGE MANGEMENT

The introduction of a new system supporting the delivery of ISS services will represent a significant change to the activities and processes that are familiar to current system stakeholders. These stakeholders include Industry, OGDs, PWGSC and ISS staff. The Contractor must manage the Change as a process at both individual and organizational level.

ISS will require the development and execution of a Change Management Strategy to ensure early, iterative and successful adoption of the new system. These services will include the identification of impacted parties and the development and delivery of an operational readiness plan, communication plan and training plan appropriate to each of these parties, including all associated deliverables, artifacts, tools and materials.

The purpose of change management is to ensure incremental and seamless transition and eventual adoption of the system being introduced, to all audiences and stakeholders.

To successfully manage change on an individual and organizational level, the Contractor should address the following:

(a) Awareness of the need for change;
(b) Desire to participate and support the change;
(c) Knowledge on how to change;
(d) Ability to implement the required skills, knowledge and behaviours;
(e) Obstacles to successfully implement change;
(f) Reinforcement to sustain the change; and
(g) State of readiness.

Effective Change Management is intended to:
(a) Avoid disruption of service to Canadians;

(b) Facilitate the adoption of process and terminology transitions for all systems users, including External and Internal Users;
(c) Ensure appropriate, accurate and timely use and input to the new system; and
(d) Ensure the quality and integrity of the services rendered.

The Contractor must plan, manage and monitor change management activities through:

(a) Explicit and elaborated early-onset Training Plans for all system stakeholders (ISS Centre of Expertise, ISS Trainers, Processors, Industry, OGDs, CIOB IT etc.);
(b) Explicit and elaborated early-onset Communications Plan appropriately tailored in frequency and content to all stakeholders;
(c) Development of training materials, self-service training packages and reference materials covering system and business processes;
(d) Early, continued and consistent inclusion and engagement of all Solution users to ensure incremental learning, familiarity, adoption and efficacy prior to system launch;
(e) Early assessment of possible change management risks, the impact of those risks and mitigation measures for insertion into the project's risk registry; and Risk Registry; and
(f) Delivery of an ongoing Change Management Report that will track current and upcoming activities and approaches to change management, as well as evaluate completed activities.

2.2 DETAILED REQUIREMENTS - CHANGE MANGEMENT

2.2.1 Change Management Approach

The Contractor must meet, but is not limited to, the following change management requirements:

Category	SOW NUM	Requirement
Change Management Approach	CM.01	The Contractor must provide a Change Management Strategy for review and approval by the Project Authority. As a minimum, the Change Management Strategy must include a high level change management strategy based on an assessment of the project, risks and stakeholders which includes: (a) Assessment to understand the: i. Change (Context of Change, Impact of Change, Change Agility [readiness]); ii. Project; iii. Change risk assessment; iv. Stakeholder identification and mapping; v. Stakeholder required knowledge/skills; and vi. Organizational changes identifying key areas of change and potential impacts. (b) Communication strategy based on identified areas of change and impacted stakeholders; (c) Training strategy based on identified areas of change and impacted stakeholders; (d) A Gap Analysis to identify required areas of Engagement, Communications and Training; (e) "Best Fit Change Strategy" that identifies the right overall concept for

Category	SOW NUM	Requirement
		delivering change based on the assessment. This should cover benefits of the approach, how to involve stakeholders, sustainability and assessment of operational readiness; (f) Discussion of transition approach based on leading practices; (g) Transitional success criteria and how transitional success will be evaluated; (h) Identification of change levers available to the project team; (i) Change resourcing expectations based on project phases and milestones; and (j) Process and Stakeholder readiness assessments tied to each go-live.

2.2.2 Change management Plan

The Contractor must provide and maintain a Change Management Plan, following the approval of the Change Management Strategy. The Change Management Plan is subject to review and approval by the Project Authority. The Project Management Plan is to be updated as the project progresses or when requested by the Project Authority. The Change Management Plan must include:

(a) A Operational Readiness Plan;
(b) Communication Plan; and
(c) Training Plan;

Category	SOW NUM	Requirement
General	CM.02	The Change Management Plan must be integrated with the Project Management Plan and Project Schedule.
	CM.03	The Contractor must: (a) Develop processes and procedures to institutionalize the change; (b) Identify change management activities and link them to project milestones (c) Align with training timelines, communications, and approaches; (d) Align with process re-engineering transition activity timelines; (e) Identify change resourcing expectations based on project phases and milestones; (f) Identify when, for how long, and the type of GC resources that are required for change management; (g) Identify high risk areas that might impact successful change, develop mitigation strategies and recommended mitigation actions, and report results to GC; (h) Identify quick wins for simplifying change management activities; (i) Work in collaboration with the GC in executing the Change Management Strategy and Plan; (j) Action change management remediation activities required throughout project lifecycle; (k) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues; (l) Support identified GC Change Management resources who will champion change; and (m) Coordination between the various components of change management and

Category	SOW NUM	Requirement
		the other project activities.
Operational Readiness Plan	CM.04	The Contractor must provide and maintain an Operational Readiness Plan for review and approval by the Project Authority, that must include, at minimum: (a) Assessment of current operations (b) Criteria for determining readiness to change (c) Assessment of readiness at the start of development (d) Reassessment of change management progress and operational readiness as the project progresses and prior to each go live; and (e) Assess remediation actions based on readiness assessments and report status to GC.
Communications Plan	CM.05	The Contractor must provide and maintain a Communication Plan for review and approval by the Project Authority, that must include, at minimum: (a) Overview of content for communication artifacts such as but not limited to: i) Communicating the benefits of the ISST project; ii) Communicating how the GC readiness activities will be accomplished; iii) Communicating how Users can support the GC; iv) Transition effort to migrate from the current AS-IS business processes and system to the future TO-BE business processes and system; 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) Description of Contractor's approach to change leadership engagement by confirming leadership buy-in, creating change advocates, providing coaching and tools for leadership's role in driving adoption; (c) Develop a change advocate network within ISS to facilitate leadership engagement for active support and driving of change; (d) Identifying communication activities throughout the lifecycle of the project, flagging any potential obstacles to initiating those activities and possible solutions; and (e) Identify an approach for soliciting and managing feedback and develop remediation action plans for areas of the change management that require improvement.
Communications Delivery	CM.06	The Contractor must: (a) Evaluate and update communication activities based on project risks and issues and provide assessment on what communication activities can assist in mitigation measures; (b) Facilitate workshops to discuss, analyze and validate changes; (c) Deliver information sessions including, but not limited to: proof of concept sessions, hands on system trials, brainstorming sessions, etc.; (d) Document feedback from communications to produce a report outlining successfulness of delivered communication activities; (e) Develop and deliver communication materials for the purpose of communication and engagement activities including, but not limited to: presentations, agenda, info brochures, stakeholder communications, etc.; (f) Reassess communication activities based on readiness assessments and report

Category	SOW NUM	Requirement
		findings and provide recommendations: and (g) The contractor must work with the GC on the execution of all communication activities with internal PWGSC stakeholders, OGDs and Industry Users.
Training Plan	CM.07	The Contractor must provide and maintain a Training Plan for review and approval by the Project Authority. (a) As a minimum, the Training Plan must describe the training approach, as well as how the Contractor will: i) Define required skills and level of skills to support the application in terms of business knowledge, application knowledge and solution knowledge; ii) Articulate how Users will be assessed to ensure they have an understanding of their roles and the solutions capabilities; iii) Identify methods, procedures and materials required for delivering training, user acceptance testing and knowledge transfer; iv) Identify an approach to collecting feedback from trainees to indicate areas where improvement is required or where success was achieved. Identifying potential areas of solution weakness or a need for training improvement; v) Determine the training requirements assessments by User type. This must address the initial, incremental and end-to-end training requirements for the Solution, as well as ongoing training requirements for new Users or refresher training; (b) As a minimum, the Training Plan for Users must: i) Include a schedule of training phases beginning early in 2018 and continuing through to March 2019; ii) Clearly outline training needs; iii) Clearly outline training delivery methods and materials specific to each user type; iv) Articulate how users will be assessed to ensure they have an understanding of their roles and system capabilities; v) Identify required skills and competency levels to support the application in terms of business knowledge, application knowledge and solution knowledge; vi) Link the communication of training activities to the Change Management Communication Plan; vii) Synchronize scheduled training activities to account for Process Re-Engineering activities; viii) Include instructions on locating training resources; ix) Detail expected User outcomes; and x) Detail instructions on each transition approach including: (1) Tools and resources that will be available; (2) How to populate User profiles; (3) Frequently asked questions; and (4) Instructions on providing feedback during the transition. (c) 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

Category	SOW NUM	Requirement
		service desk agents during the GC migration; iii) Instructions on locating training resources; and iv) Escalation procedures. (d) 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; and iii) Instructions on locating training resources.
Training Delivery	CM.08	The Contractor must perform the following activities which includes thorough technical and User training, effective communication and successful stakeholder participation: (a) Delivery of process oriented end to end standard operating procedures outlining key activities and user responsibility so that end users are informed as to the changes to their day to day activities; (b) Delivery of training materials that ensure: i) The right skills are provided to operate the new solution (ISS processors and industry users); and ii) The right skills are provided to support/maintain the new solution (ISS system administrators and CIOB/SSC). (c) Document feedback from trainees and to produce a report outlining successfulness of delivered training; (d) 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; (e) 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; (f) Conduct training for External Users, including selected virtual or computer-based training and reference materials for Users enabled in the Solution; (g) Conduct Internal User training, including selected classroom-style and computer-based training, including new employee training, upgrade classes and specific skills; (h) Conduct Train the Trainer training for Users as defined by GC; (i) 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; (j) Inform and train Users about the end-to-end solution that will support their business requirements; (k) Provide the training materials to be used within the SABA learning management delivery service; (l) Demonstrate successful training by having users or groups of users complete a predetermined process in its entirety (m) Develop, document and deliver a training program to instruct GC personnel on all aspects of the Solution processes and functionalities; (n) Develop, document and deliver content for training modules that are copyright and royalty free for modification and redistribution by the GC; and

Category	SOW NUM	Requirement
		(o) The Contractor must facilitate and deliver all initial and ongoing training to the GC and industry over the course of the Contract.
Official Languages	CM.09	All instructions, training, communication, role descriptions that are intended for Internal and External Users must be available and presented in the user's Official Language of choice.

SECTION 8: SOLUTION SUSTAINMENT

This section defines the requirements for the sustainment of the Solution.

1.1 REQUIREMENT OVERVIEW

The Contractor is responsible for the design and development of materials, processes and activities that will be used by both the ISS Center of Expertise and PWGSC CIOB/SSC for the ongoing support and maintenance of the Solution once the Solution has been released. The Contractor is expected to ensure that the ISS Center of Expertise is ready and capable to offer post release Solution training and support services to Internal and External Users. The Contractor is also required to ensure that both PWGSC CIOB and SSC are able to provide the required technical support.

1.2 DETAILED REQUIREMENTS

The Contractor is required to meet the following Solution sustainment requirements:

Category	SOW NUM	Requirement
Solution Sustainment	SS.01	Develop full system documentation including both technical and functional aspects of the solution.
	SS.02	Develop new system and processes diagrams that depict the relationships between system components and between the system and the various users.
	SS.03	Delivery of process oriented end to end standard operating procedures outlining key activities and user responsibility so that end users are informed as to the changes to their day to day activities.
	SS.04	Develop, document and deliver a GC-accessible knowledge database.
	SS.05	Develop a system administration handbook on how to properly administer the system.
	SS.06	Develop ongoing information dissemination strategy for system.
	SS.07	Develop set of processes to ensure the change is adopted and sustained in the long term.
	SS.08	Assist in the development of system support processes.
	SS.09	Document and present recommendations for future enhancements

SECTION 9: OPTIONAL SERVICES

The Work described in this section will be requested by GC through a Task Authorization on an as-and-when-requested basis using the Task Authorization Form at ANNEX E. The basis of payment for any Task Authorization will be specified at the time of request.

1.1 ADDITIONAL BUSINESS PROCESS RE-ENGINEERING SERVICES

In addition to the Business Process Re-Engineering services described in Section 2: 1.1 and 1.2, the Contractor must, on an as-and-when requested basis, provide additional Business Process Re-Engineering services and must propose resources that are qualified and have experience providing Business Process Re-Engineering services.

1.2 ADDITIONAL DATA MIGRATION SERVICES

In addition to the Data Migration services described in Section 2: 2.2.3 Data Migration, the Contractor must, on an as-and-when-requested basis, provide additional Data Migration services and must propose resources that are qualified and have experience providing Data Migration services.

1.3 ADDITIONAL SYSTEM DEVELOPMENT AND CONFIGURATION

While the Statement of Work clearly defines a flexible Solution that can be configured by GC, the GC may have a requirement to modify the Solution to accommodate changes in the operational and security environment, and may request additional services in support of these changes to the system configuration.

In addition to the services described in Section 2: Business Requirements, Section 3: Technical Requirements, Section 4: Secure Access, and Section 5: IT Security Requirements, the Contractor must, on an as-and-when-requested basis, provide additional System Development and Configuration services and must propose resources that are qualified and have experience providing System Development and Configuration services.

1.4 ADDITIONAL TESTING MANAGEMENT SERVICES

In addition to the Testing Management services described in Section 6: Testing Management, the Contractor must, on an as-and-when-requested basis, provide additional Testing Management services and must propose resources that are qualified and have experience providing Testing Management services.

1.5 ADDITIONAL PROJECT MANAGEMENT AND CHANGE MANAGEMENT SERVICES

In addition to the Project Management and Change Management services described in Section 7: Management and Oversight, the Contractor must, on an as-and-when-requested basis, provide additional Project Management and Change Management services and must propose resources that are qualified and have experience providing Project Management or Change Management services.

1.6 ADDITIONAL SOLUTION SUSTAINMENT SERVICES

In addition to the Solution Sustainment services described in Section 8: Solution Sustainment, the Contractor must, on an as-and-when-requested basis, provide additional Solution Sustainment services and must propose resources that are qualified and have experience providing Solution Sustainment services.

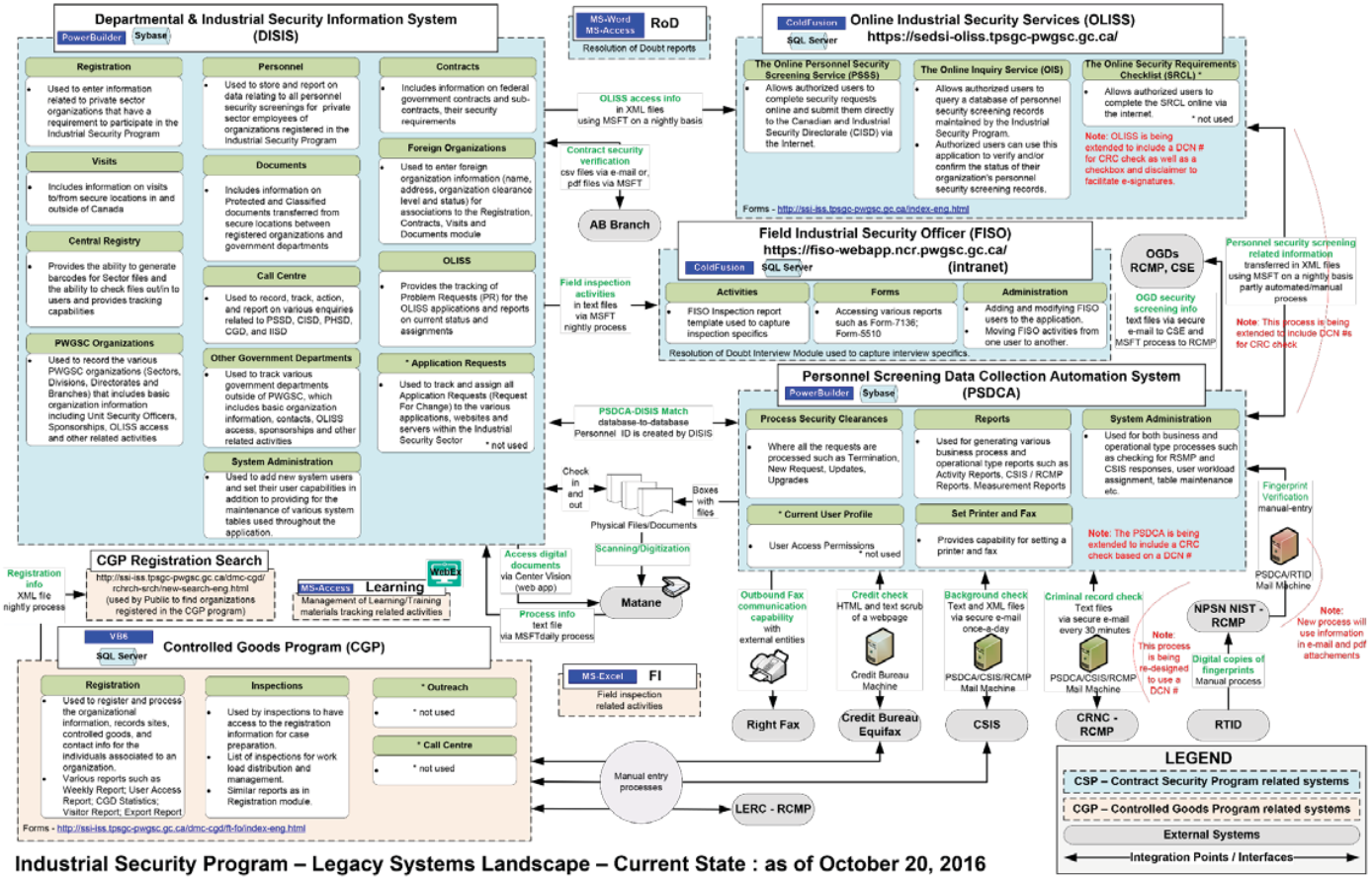
1.7 PROFESSIONAL SERVICES CATEGORIES

For the optional services described in accordance with Section 9: 1.1 Additional Business Process Re-Engineering Services, 1.2 Additional Data Migration Services, 1.3 Additional System Development and Configuration Services, 1.4 Additional Testing Management Services, 1.5 Additional Project Management and Change Management Services, 1.6 Additional Solution Sustainment Services, the Contractor must provide the professional services outlined in ANNEX F – Resource Category Information for Optional Services, in accordance with the All Inclusive Per-Diem Rates as per ANNEX B – Price Schedule, 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.

APPENDIX 1 TO ANNEX A – CURRENT BUSINESS PROCESSES

APPENDIX 1 TO ANNEX A – CURRENT BUSINESS PROCESSES

This Appendix outlines current business processes for delivering Contract Security Program and Controlled Goods Program.



Industrial Security Program – Legacy Systems Landscape – Current State : as of October 20, 2016

1.1 CONTRACT SECURITY PROGRAM BUSINESS PROCESSES

1.1.1 Contract Security - Pre-Contract Award

The contract security pre contract award business process supports government procurement function by ensuring security in contracts awarded by Public Works and Government Services Canada (PWGSC) or when requested by other government departments. The security requirements associated with a protected/classified contract are identified on a Security Requirements Check List (SRCL), and are issued with bid solicitation documents and maybe amplified by security clause(s) included in the contract document. In the case of international contracts, the Contract Security Program (CSP) will liaise with the responsible foreign government to receive security assurance prior to the release of protected/classified information or assets to foreign interests.

Supplied SRCL and supporting contract documentation are reviewed to ensure they are complete. Revised or updated SRCL's can trigger other CSP processes. Sub contract SRCL's require the primary contract be approved before the sub contract can be placed for RFP. Identified foreign bidders as a result of the RFP process may require an updated SRCL to obtain any foreign security clauses.

The contracting authority is provided with contract security clauses based on information provided in the submitted SRCL. Typically security clauses are domestic in nature but can also include foreign security clauses. Provisioned security clauses are included in the contracts solicitation documentation. Thus preventing unauthorized access to Protected/Classified information and assets.

The CSP makes sure Canadian organizations have appropriate safeguarding measures in place for contracts with foreign countries. If requested by foreign governments, the CSP can provide assurances to confirm the security clearances of Canadian organizations wishing to bid on sensitive foreign contracts. Similarly the CSP can request from foreign governments assurance that foreign organizations have appropriate safeguarding.

Workflow ID	**1 WF CSP Contract Pre Award**
Business Unit(s)	• Client Contract Authority • Industrial Security Sector Contract Security Program – Contract Analyst
Business Objective	• Submission of SRCL by Contracting Authority for analysis and provision of security clauses. • Security clauses are required for inclusion in the contract's Request for Proposal.
Trigger	• Contract with the Government of Canada that has identified security requirements.
Workflow Description	1. Start of process. 2. Client contract authority identifies that the contract has possible security requirements. 3. Client contract authority provides supporting documentation as required.

	4. Client contract authority completes and submits a Security Requirements Check List (SRCL) to the Industrial Security Sector's, Contract Security Program (CSP). If there is an existing SRCL and contract, the client contract authority would submit a sub-SRCL as part of a sub contract. 5. CSP receives the SRCL and performs a triage to determine if the submitted SRCL is new, a revision to an existing or a sub-SRCL. 6. If it is a new SRCL, a new entry is created into the existing supporting application. Go to step 16. 7. If it is revision to an existing SRCL, the existing SRCL and contract information is retrieved. Go to step 16. 8. If is a sub-SRCL the CSP will validate that the primary contract exists and is at the appropriate security level. 9. If the sub-SRCL's primary contract does not exist, the sub-SRCL is rejected. 10. The client authority who submitted the sub-SRCL is notified of the rejection. Go to step 15. 11. If the sub-SRCL's primary contract does exist, the CSP will confirm if the primary contract has been approved. 12. If the sub-SRCL's primary contract has not been approved, the contract authority and company security officer (CSO) are notified. 13. If required the sub-SRCL will trigger either a new registration or registration upgrade process (3 WF CSP Registration New/Upgrade), otherwise go to step 15. 14. If the sub-SRCL's primary contract has been approved, the contract authority is notified. Depending on the specifics of the contract, other interested stakeholders such as Communications Security Establishment Canada (CSEC), ISS Controlled Goods Program (CGP), etc. are also notified. A site inspection may also be triggered if required. The SRCL and contract are flagged for follow up. 15. The contract pre award process ends. 16. The CSP reviews the submitted SRCL and any supplied supporting documentation. 17. The CSP reviews the submitted SRCL for completeness. 18. If the SRCL is not complete, the client authority is notified that the SRCL needs to be revised. The process starts over at step 4. 19. If the SRCL is complete, the CSP identifies the required domestic security clauses based on the contracts security requirements. 20. If the SRCL indicates there are foreign security requirements. The International Industrial Security Directorate (IISD) is consulted. 21. The IISD identifies the required foreign security clauses and supplies them back to the CSP. 22. The CSP returns all identified security clauses to the client authority for inclusion into the contract's RFP. 23. If the security clauses were provided for a revised SRCL, interested stakeholders such as Communications Security Establishment Canada (CSEC), ISS Controlled Goods Program (CGP), etc. are notified. A site inspection may also be triggered if required. The SRCL and contract are flagged for follow up. 24. The client authority adds the supplied security clauses to the contract solicitation documentation. 25. The contract is placed for RFP. 26. Contract potential bidders are identified. 27. If there are no potential foreign bidders, go to step 29.

	28. If there are potential foreign bidders, the contract and its SRCL is reviewed for foreign security clauses to ensure contract security. 29. The Post Contract Award process (2 WF CSP Contract Post Award) is triggered.
Inputs	• Security Requirements Check List (SRCL)
Outputs	• Domestic and foreign security clauses • Stakeholder notifications

1.1.2 Contract Security - Contract Post Award

The post contract award process reviews submitted contract information confirming Government Security Policy (GSP) compliance by determining if required security clauses were included in the contract, contract awarded organization is registered with the CSP and has the appropriate level of security per the contract security requirements. Other CSP processes can be triggered as a result of the post contract award review process. Should all security requirements of the contract be met, the contract authority will be advised to process the contract.

The subcontracting is used when a primary contract holder requires work to be done by another organization. A subcontract is to be reported to the CSP for approval when there are security requirements. International subcontracting requires the CSP to confirm the security status of the foreign organization prior to any commercial commitment. Each subcontract requires its own SRCL for approval and will obtain subcontract specific contract security clauses for inclusion within the subcontract. The subcontract security cannot be higher than that of the prime contract but could be lower if required.

Workflow ID	**2 WF CSP Contract Post Award**
Business Unit(s)	• Contract Authority • Industrial Security Sector Contract Security Program – Contract Analyst
Business Objective	• Review of submitted contracts confirming Government Security Policy compliance.
Trigger	• Awarded contract with the Government of Canada that has identified security requirements.
Workflow Description	1. Start of process. 2. Client contract authority submits contract information to CSP. Contract information can be supplied directly from contract authority or from the Automated Buyers Environment System (ABE). 3. The CSP reviews the submitted contract information for completeness.

	4. If the information is not complete, the CSP will request the information from the contract authority. 5. If the supplied information is complete, the CSP verifies if the contract is compliant. 6. If compliant go to step 23. If not compliant one of four (step 7, step 9, step 12 or step 15) processes could be triggered. As they are situation dependent it is possible for one or more processes to be triggered based on the non-compliancy reasons. If the foreign security clauses are missing or there is an issue with the awarded foreign contractor, the IISD is consulted. 7. If the security clauses are missing from the contract. 8. The CSP contacts the client contract authority advising of required action. Go to step 30. 9. If there is a noted security breach, the CSP will check with the client contract authority for breach mitigations. 10. If the CSP is satisfied with the client contract authority response, go to step 30. 11. If the CSP is not satisfied with the client contract authority response, an investigation is triggered (12 WF CSP Investigations). Go to step 30. 12. If the awarded contractor requires to be registered with the CSP. 13. The client contract authority is notified that the contracting organization needs to be registered. 14. The CSP registration process is triggered (3 WF CSP Registration New/Upgrade). Go to step 18. 15. If the awarded contractor is already registered but requires an upgrade to their security clearance level. 16. The CSP will initiate the organization registration upgrade process on behalf of the client or the CSP will advise the client to initiate the PSOS. 17. The CSP registration upgrade process is triggered (3 WF Registration New/Upgrade). Go to step 18. 18. If the contracting organization is found to be compliant as part of the registration process, go to step 23. 19. If the contracting organization is found not to be compliant as part of the registration process, the CSP will follow-up on the contract. 20. If all compliancy issues were resolved, go to step 23. 21. If all compliancy issues were not resolved, after a predetermined number of attempts with no response, the contract is closed-out. 22. An investigation is triggered (12 WF CSP Investigations). Go to step 30. 23. Interested stakeholders such as Communications Security Establishment Canada (CSEC), ISS Controlled Goods Program (CGP), etc. are notified of the contract award. 24. If the contract has inspection requirements such as an IT inspection. If there are no inspection requirements go to step 28. 25. The contract analyst will initiate an inspection 26. The inspection process occurs (10 WF CSP Inspection). 27. If the inspection process identified any issues, the contract is followed up on. 28. If identified issues were not resolved, the contract is followed up on again, this cycle continues until all inspection identified issues are resolved. 29. If all identified issues are resolved, the client contract authority is advised to proceed with the processing of the contract. 30. The process ends.
Inputs	• Security Requirements Check List (SRCL) • Awarded contract and supplemental information

	• Investigation results • Inspection results • Organization Registration New or Upgrade
Outputs	• Close out of contract for non-compliancy • Stakeholder notifications • Contract award and processing

1.1.3 Registration in Contract Security Program - New/Upgrade

The organizational security screening services supports the registration of companies wishing to participate in a Government of Canada (GC) and foreign government contracts with security requirements. The CSP conducts security screening of registered Canadian private sector organizations to ensure that organizations have implemented appropriate security safeguards for the handling of protected/classified GC information and assets. Organizations are required to have an organization security clearance prior to beginning work on GC contract with security requirements. The CSP verifies and/or initiates clearances with foreign partners to provide assurances that companies abroad meet the security requirements of GC contracts

The organization registration business process involves the receipt and evaluation of registration requests against specified secured contracts. Subcontracted organizations require the prime contractor to already have been registered. Organizations that are unable to meet the registration requirements are closed out for non-compliance.

Workflow ID	**3 WF CSP Registration New/Upgrade**
Business Unit(s)	• Sponsoring Organization • CSP Contract Analyst • CSP Registration Clerk • CSP Registration Analyst
Business Objective	• To perform security screening of new registered organizations to ensure contract security. • To perform an upgrade security screening of registered organizations to ensure contract security.
Trigger	• Sponsoring organization submits a request to have another organization registered or to have their existing security clearance upgraded. • CSP Contract Analyst triggers the registration process.

Workflow Description	1. Start of process. 2. Sponsoring organization or CSP contract analyst submits a request to register a new organization or upgrade an existing organization. 3. CSP registration clerk verifies if the organization already exists within the contract security program. 4. If the organization already exists, the CSP registration clerk verifies if the requested security level is greater than the organizations current security level. 5. If the requested security level is not greater than the organizations current security level. The sponsor is notified that the sponsored organization is already registered. Go to step 8. 6. If the organization does not already exist within the CSP OR the requested organization security level is greater than the exiting security level, the sponsor type is observed. 7. If the sponsor is from industry, the CSP registration clerk will verify if sponsor is the prime contractor who is sponsoring a sub-contractor. If not, go to step 8. 8. The sponsor is sent a rejection letter. 9. The registration request is closed-out. 10. If the sponsor is from another government department (OGD) OR the sponsor is the primary contractor, the CSP registration clerk reviews, prioritizes and assigns organization registration request to a CSP registration analyst. 11. CSP registration analyst reviews the registration package. If the registration package is complete, go to step 17. 12. If the registration package is not complete, the requested organizational security level is reviewed and an establishing letter is sent to the organization requesting information. 13. If the documentation is provide within 30 business days, go to step 17. 14. If the requested documentation is not provided within 30 business days, a follow-up on the establishing letter is sent to the organization. 15. If the requested documentation is provided within 5 business days, go to step 17. 16. If the requested documentation is not provided by the organization within the 5 business days, the registration request is closed-out for non-compliance. 17. The CSP registration analyst reviews and validates all provided information. 18. If the organization security clearance is for a Designated Organizational Screening (DOS). 19. The DOS security clearance process is triggered (4 WF CSP Registration DOS). 20. If the organization security clearance is for Facility Security Clearance (FSC). 21. The FSC security clearance process is triggered (5 WF CSP Registration FSC). 22. If the organization security clearance is for Document Safeguarding Capability (DSC). 23. The FSC security clearance process is triggered (6 WF CSP Registration DSC). 24. The registration new/upgrade process ends.
Inputs	• PSOS • Supplied organization information
Outputs	• Establishing letter • Rejection letter

	• Close-out notification

1.1.4 Registration in Contract Security Program - Organization Security Screening

The Organization registration security screening business processes evaluates the organization based on the security level specified in the secured contract and a need to know requirement. The security screening evaluates organizational structure, ownership, legal status, Key Senior Officials (KSOs), Company Security Officer (CSO), physical security and information technology security safeguards, etc. Organizations that meet the contracts security requirements for Canadian and/or foreign government information/assets are granted their requested organizational security clearance, such as Designated Organizational Screening (DOS), Facility Safeguarding Capability (FSC), Document Safeguarding Capability (DSC), etc.

Organizations that are unable to provide the required information are closed out for non-compliance or their organization security clearance level downgraded. Depending on the required organization security clearance level, other CSP processes can be triggered.

1.1.4.1 Designated Organizational Screening

Workflow ID	4 WF CSP Registration DOS
Business Unit(s)	• CSP Registration Analyst • CSP Registration Quality Assurance Officer • CSP Registration Chief
Business Objective	• To clear an organization at the DOS security clearance level.
Trigger	• New or upgrade registration request. • FSC or DSC registration request.
Workflow Description	1. Start of process. 2. CSP registration analyst confirms that all required information is received. 3. If not all information is received, the CSP registration analyst determines if there is a need to request the information. If there is a need, the organization is contacted, go to step 2. If the CSP registration analyst determines that the file is to be closed out, go to step 13. 4. If all the requested information has been received, the CSP registration analyst determines if there is a need to request a personnel security screening (PSS). If no PSS is required, go to step 9. 5. If PSS is required, the CSP registration analyst will create and send a registration package to the Personnel Security Screening Division (PSSD) of the CSP requesting personnel security screenings for identified organizational individuals.

	6. The PSS process is triggered (13 WF CSP PSS Request). 7. The registration package is returned from PSSD and the PSS results are reviewed. 8. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 5. 9. If there were no issues with the PSS results, the CSP registration analyst confirms if there is a need to terminate the organization. If there is no need to terminate the organization go to step 14. 10. If there is a need to terminate the organization, the CSP registration analyst reviews the organization to determine if there is anything that would prevent the termination, for example is the organization currently involved in an active contract. If there is something that would prevent the termination of the organization, go to step 3. 11. If there is nothing preventing the organization termination, as required all PSS clearances are terminated. 12. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination. 13. The registration request is closed-out for non-compliance. Go to step 21. 14. CSP registration analyst creates the notification of registration. 15. The file is submitted to the CSP quality assurance officer for review. 16. CSP quality assurance officer reviews the file. 17. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates. 18. CSP registration analyst updates the file, go to step 15. 19. If the CSP quality assurance officer determines no modifications are required, the CSP registration chief is requested to sign off on the granting letter. 20. CSP registration analyst notifies the organization's CSO and sponsor. The notification includes the organization clearance letter, PSS briefing forms, 3G security agreement and organizational security status. 21. The trigger for the DOS can trigger other registration processes. 22. Where required, the Facility Security Clearance (FSC) or Document Safeguarding Capability (DSC) would be triggered (5 WF CSP Registration FSC or 6 WF CSP Registration DSC). 23. Where required, the new or upgrade registration process may be triggered (3 WF CSP Registration New/Upgrade).
Inputs	• PSOS • Establishing letter • Supplied organization information • PSSD results
Outputs	• Termination notice • PSSD registration package • Granting letter • Organization clearance letter • PSS briefing forms • 3G security agreement • Organizational security status

1.1.4.2 **Facility Safeguarding Capability**

Workflow ID	**5 WF CSP Registration FSC**
Business Unit(s)	• CSP Registration Analyst • CSP Registration Quality Assurance Officer • CSP Registration Chief
Business Objective	• To clear an organization at the FSC security clearance level.
Trigger	• New or upgrade registration request. • DOS registration request.
Workflow Description	1. Start of process. 2. CSP registration analyst reviews to determine if DOS security clearance needs to be processed. If there is no need to process a DOS, go to step 4. 3. If there is a requirement to process a DOS security clearance, the DOS clearance process is triggered (4 WF CSP Registration DOS). 4. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 8. 5. If there are organizational changes the CSP registration analyst reviews in detail the organization. 6. CSP registration analyst performs a call briefing with the organizations CSO. 7. The CSP registration analyst completed a 1A Requirements report. 8. CSP registration analyst verifies that all information is received. 9. If not all information is received, the CSP registration analyst determines if there is a need to request the information. If there is a need, the organization is contacted, go to step 8. If the CSP registration analyst determines that the file is to be closed out, go to step 19. 10. If all the requested information has been received, the CSP registration analyst determines if there is a need to request a personnel security screening (PSS). If no PSS is required, go to step 15. 11. If PSS is required, the CSP registration analyst will create and send a registration package to the Personnel Security Screening Division (PSSD) of the CSP requesting personnel security screenings for identified organizational individuals. 12. The PSS process is triggered (13 WF CSP PSS Request). 13. The registration package is returned from PSSD and the PSS results are reviewed. 14. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 11. 15. If there were no issues with the PSS results, the CSP registration analyst confirms if there is a need to terminate the organization. If there is no need to terminate the organization go to step 20.

	16. If there is a need to terminate the organization, the CSP registration analyst reviews the organization to determine if there is anything that would prevent the termination, for example is the organization currently involved in an active contract. If there is something that would prevent the termination of the organization, go to step 9. 17. If there is nothing preventing the organization termination, as required all PSS clearances are terminated. 18. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination. 19. The registration request is closed-out for non-compliance or the security clearance is downgraded to DOS. Go to step 27. 20. CSP registration analyst creates the notification of registration. 21. The file is submitted to the CSP quality assurance officer for review. 22. CSP quality assurance officer reviews the file. 23. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates. 24. CSP registration analyst updates the file, go to step 21. 25. If the CSP quality assurance officer determines no modifications are required, the CSP registration chief is requested to sign off on the granting letter. 26. CSP registration analyst notifies the organization's CSO and sponsor. The notification includes the organization clearance letter, PSS briefing forms, 3G security agreement and organizational security status. 27. The trigger for the FSC can trigger other registration processes. 28. Where required, a Document Safeguarding Capability (DSC) would be triggered (6 WF CSP Registration DSC). 29. Where required, the new or upgrade registration process may be triggered (2 WF CSP Registration New/Upgrade).
Inputs	• PSOS • Establishing letter • Supplied organization information • PSSD results
Outputs	• Termination notice • PSSD registration package • Granting letter • Organization clearance letter • PSS briefing forms • 3G security agreement • Organizational security status

1.1.4.3 **Document Safeguarding Capability**

Workflow ID	**6 WF CSP Registration DSC**
Business Unit(s)	• CSP Registration Analyst • Canadian Industrial Security Directorate (CISD) Director
Business Objective	• To clear an organization at the DSC security clearance level.
Trigger	• New or upgrade registration request. • DOS registration request.
Workflow Description	1. Start of process. 2. CSP registration analyst reviews to determine if DOS security clearance needs to be processed. If there is no need to process a DOS, go to step 4. 3. If there is a requirement to process a DOS security clearance, the DOS clearance process is triggered (4 WF CSP Registration DOS). 4. CSP registration analyst determines if a FSC security clearance needs to be processed. If there is no need to process a FSC, go to step 6. 5. If there is a requirement to process a FSC security clearance, the FSC clearance process is triggered (5 WF CSP Registration FSC). 6. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 9. 7. If there are organizational changes the CSP registration analyst reviews in detail the organization. 8. CSP registration analyst performs a call briefing with the organizations CSO. 9. CSP registration analyst determines if parent exclusion is required. If no parent exclusion is required, go to step 13. 10. If there is parent exclusion, the CSP analyst requests additional information from the organization. 11. CSP registration analyst reviews and analyzes the received information. 12. Approval of the organization's parent exclusion is provided by the CISD director. 13. CSP registration analyst verifies that all information is received. 14. If not all information is received, the CSP registration analyst determines if there is a need to request the information. If there is a need, the organization is contacted, go to step 13. If the CSP registration analyst determines that the file is to be closed out, go to step 24. 15. If all the requested information has been received, the CSP registration analyst determines if there is a need to request a personnel security screening (PSS). If no PSS is required, go to step 20.

	16. If PSS is required, the CSP registration analyst will create and send a registration package to the Personnel Security Screening Division (PSSD) of the CSP requesting personnel security screenings for identified organizational individuals. 17. The PSS process is triggered (3 WF CSP PSS Request). 18. The registration package is returned from PSSD and the PSS results are reviewed. 19. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 16. 20. If there were no issues with the PSS results, the CSP registration analyst confirms if there is a need to terminate the organization. If there is no need to terminate the organization go to step 25. 21. If there is a need to terminate the organization, the CSP registration analyst reviews the organization to determine if there is anything that would prevent the termination, for example is the organization currently involved in an active contract. If there is something that would prevent the termination of the organization, go to step 14. 22. If there is nothing preventing the organization termination, as required all PSS clearances are terminated. 23. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination. 24. The registration request is closed-out for non-compliance. Go to step 27. 25. CSP registration analyst creates an inspection request. 26. The inspection process is triggered (10 WF CSP Inspection). 27. Where required, the new or upgrade registration process may be triggered (3 WF CSP Registration New/Upgrade).
Inputs	• PSOS • Establishing letter • Supplied organization information • PSSD results
Outputs	• Termination notice • PSSD registration package • Granting letter • Organization clearance letter • PSS briefing forms • 3G security agreement • Organizational security status

1.1.5 Registration in Contract Security Program - Renewal

The registration renewal business process involves the identification and notification to organizations when their organization security clearance is expiring. Renewal cycles vary between the different organizational security clearance types. An organization's renewal information is received, reviewed and evaluated

for determination if the organization still requires the existing organization security clearance. Failure to renew the organization security clearance can result in the organization security clearance to be revoked or terminated.

Workflow ID	7 WF CSP Registration Renewal
Business Unit(s)	• Registered Organization • Registration Clerk • CSP Registration Analyst • CSP Registration Quality Assurance Officer • CSP Registration Chief
Business Objective	• To renew an organizations security clearance.
Trigger	• Organization renewal requirement.
Workflow Description	1. Start of process. 2. CSP registration clerk pulls report of expiring organizations. 3. CSP registration clerk notifies organization of renewal requirement. 4. Registered organization submits renewal information. 5. CSP registration clerk reviews, prioritizes and assigns request to registration analyst. 6. CSP registration clerk determines if to continue with renewal. If there is a need to continue, go to step 8. 7. If there is no need to continue with the renewal, close out the request for non-compliance. 8. CSP registration analyst reviews and validates the renewal information. 9. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 15. 10. If there are organizational changes the CSP registration analyst reviews in detail the organization. 11. CSP registration analyst determines if there are any DSC requirements. If there are not any DSC requirements, go to step 14. 12. CSP registration analyst submits an inspection request. 13. The inspection process is triggered (10 WF CSP Inspection). 14. CSP registration analyst performs a call briefing with the organizations CSO. 15. CSP registration analyst verifies that all information is received. 16. If not all information is received, the CSP registration analyst determines if there is a need to request the information. If there is a need, the organization is contacted, go to step 15. If the CSP registration analyst determines that the file is to be closed out, go to step 26. 17. If all the requested information has been received, the CSP registration analyst determines if there is a need to request a personnel security screening (PSS). If no PSS is required, go to step 22. 18. If PSS is required, the CSP registration analyst will create and send a registration package to the Personnel Security Screening Division (PSSD) of the CSP requesting personnel security screenings for identified organizational individuals.

	19. The PSS process is triggered (13 WF CSP PSS Request). Go to step 34. 20. The registration package is returned from PSSD and the PSS results are reviewed. 21. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 18. 22. If there were no issues with the PSS results, the CSP registration analyst confirms if there is a need to terminate the organization. If there is no need to terminate the organization go to step 26. 23. If there is a need to terminate the organization, the CSP registration analyst reviews the organization to determine if there is anything that would prevent the termination, for example is the organization currently involved in an active contract. If there is something that would prevent the termination of the organization, go to step 16. 24. If there is nothing preventing the organization termination, as required all PSS clearances are terminated. 25. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination. 26. The registration request is closed-out for non-compliance or the security clearance is downgraded to DOS. Go to step 34. 27. CSP registration analyst creates the notification of renewal. 28. The file is submitted to the CSP quality assurance officer for review. 29. CSP quality assurance officer reviews the file. 30. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates. 31. CSP registration analyst updates the file, go to step 28. 32. If the CSP quality assurance officer determines no modifications are required, the CSP registration chief is requested to sign off on the granting letter. 33. CSP registration analyst notifies the organization's CSO and sponsor. The notification includes the organization clearance letter, PSS briefing forms, 3G security agreement and organizational security status. 34. The process ends.
Inputs	• Renewal information • PSSD results
Outputs	• Termination notice • Granting letter • Organization clearance letter • PSS briefing forms • 3G security agreement • Organizational security status

1.1.6 Registration in Contract Security Program - Update

The registration update business process involves the submission of information to the CSP from the organization for the purpose of simply updating their information with the CSP. This business process is the same as the registration renewal business process with the difference that the submission of information is voluntary. An organization's updated information is received, reviewed and evaluated for determination if the organization still requires the existing organization security clearance. Failure to renew the organization security clearance can result in the organization security clearance to be revoked or terminated.

Workflow ID	8 WF CSP Registration Update
Business Unit(s)	• Sponsoring Organization • CSP Contract Analyst • Registered Organization • CSP Registration Clerk • CSP Registration Analyst • CSP Registration Quality Assurance Officer • CSP Registration Chief
Business Objective	• To update an organizations information for security clearance.
Trigger	• Organization update requirement.
Workflow Description	1. Start of process. 2. Sponsoring organization or CSP contract analyst submits update to an organization's information. 3. Registered organization submits an update to their information. 4. CSP registration clerk reviews, prioritizes and assigns request to registration analyst. 5. CSP registration clerk determines if to continue with update. If there is a need to continue, go to step 8. 6. If there is no need to continue with the update, reject the update request. 7. CSP registration clerk notifies the CSO of the rejected update. Go to step 34. 8. CSP registration analyst reviews and validates the update information. 9. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 15. 10. If there are organizational changes the CSP registration analyst reviews in detail the organization. 11. CSP registration analyst determines if there are any DSC requirements. If there are not any DSC requirements, go to step 14. 12. CSP registration analyst submits an inspection request.

	13. The inspection process is triggered (10 WF CSP Inspection). Go to step 34. 14. CSP registration analyst performs a call briefing with the organizations CSO. 15. CSP registration analyst verifies that all information is received. 16. If not all information is received, the CSP registration analyst determines if there is a need to request the information. If there is a need, the organization is contacted, go to step 15. If the CSP registration analyst determines that the file is to be closed out, go to step 26. 17. If all the requested information has been received, the CSP registration analyst determines if there is a need to request a personnel security screening (PSS). If no PSS is required, go to step 22. 18. If PSS is required, the CSP registration analyst will create and send a registration package to the Personnel Security Screening Division (PSSD) of the CSP requesting personnel security screenings for identified organizational individuals. 19. The PSS process is triggered (13 WF CSP PSS Request). 20. The registration package is returned from PSSD and the PSS results are reviewed. 21. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 18. 22. If there were no issues with the PSS results, the CSP registration analyst confirms if there is a need to terminate the organization. If there is no need to terminate the organization go to step 27. 23. If there is a need to terminate the organization, the CSP registration analyst reviews the organization to determine if there is anything that would prevent the termination, for example is the organization currently involved in an active contract. If there is something that would prevent the termination of the organization, go to step 16. 24. If there is nothing preventing the organization termination, as required all PSS clearances are terminated. 25. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination. 26. The registration request is closed-out for non-compliance. Go to step 34. 27. CSP registration analyst updates the organization information. 28. The file is submitted to the CSP quality assurance officer for review. 29. CSP quality assurance officer reviews the file. 30. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates. 31. CSP registration analyst updates the file, go to step 28. 32. If the CSP quality assurance officer determines no modifications are required, the CSP registration chief is requested to sign off on the granting letter. 33. CSP registration analyst notifies the organization's CSO and sponsor. The notification includes the organization clearance letter, PSS briefing forms, 3G security agreement and organizational security status. 34. The process ends.
Inputs	• Update information • PSSD results
Outputs	• Termination notice • Granting letter

	• Organization clearance letter • PSS briefing forms • 3G security agreement • Organizational security status

1.1.7 Registration in Contract Security Program - Termination

The registration termination business process is the receipt of an organization termination request, review and evaluation of the termination request, termination of the organization and its employee's personnel security clearances and finally a communique to the organization informing of the termination. Termination requests can be submitted from either the sponsoring organization, the organization itself or the CSP. Termination requests that are received are first reviewed to see if there is anything that might prevent the termination such as an open contract or if the organization had a DSC security clearance and documents were stored onsite.

Workflow ID	**9 WF CSP Registration Termination**
Business Unit(s)	• Sponsoring organization • Registered Organization • CSP Registration Analyst
Business Objective	• To terminate an organizations security clearance.
Trigger	• Organization termination requirement.
Workflow Description	1. Start of process. 2. Sponsoring organization submits a request to terminate the sponsored organization. 3. Alternate start to process. 4. The registered organization submits a request to terminate their organization. 5. Alternate start to process. 6. The CSP registration clerk submits a request to terminate an organization. 7. CSP registration analyst reviews information and analyzes the termination request. 8. CSP registration analyst determines if there are any DSC requirements. If there are not any DSC requirements, go to step 9. 9. CSP registration analyst submits an inspection request. 10. The inspection process is triggered (10 WF CSP Inspection). Go to step 14. 11. CSP registration analyst terminates the organization.

	12. CSP registration analyst terminates any PSS requests. 13. CSP registration analyst notifies the CSO and sponsor of termination. 14. The process ends.
Inputs	• Termination request
Outputs	• Organization termination

1.1.8 Registration in Contract Security Program - Inspection

The registration inspection business process conducts physical and information technology security reviews of organizations to assess and ensure that the organization is compliant with industrial security requirements, that information technology security requirements are met, levels of DSC are appropriate, alignment of company and contract information as required and to provide advice and guidance to CSO's on security requirements.

Workflow ID	**10 WF CSP Inspection**
Business Unit(s)	• Organization Representative • CSP Inspector • CSP Senior Inspector • CSP Inspection Manager • CSP Registration/Contracts
Business Objective	• Conduct physical and information technology security reviews of an organization to assess and ensure: o Organizations are compliant to industrial security requirements. o Information technology security requirements are met. o Level of DSC is appropriate. o Alignment of company and contract information to ensure that all information meets established quality standards. o Provide advice and guidance to CSO's on security requirements.
Trigger	• Various triggers from other workflows.
Workflow Description	1. Start of process. 2. Registration workflow (3 WF CSP Registration New/Upgrade). 3. Contract post award workflow (2 WF CSP Contracts Post Award). 4. DCS Renewal workflow (6 WF CSP Registration DSC). 5. The Senior Inspector review the inspection request. 6. Decision: Is documentation for inspection request complete? [Yes: Step 8, No: Step 6].

	7. The senior inspector request missing information from requestor, which could be from Registration or Contract division 8. Registration analyst or Contract specialist provide the missing inspection details to Senior Inspector. 9. The Senior Inspector determines whether the inspection should take place onsite (this applies to physical and IT inspections) or can be done offsite (when a phone interview is all that is required). 10. The Senior Inspector organize which inspector should be assigned to the request based on region, availability and expertise of inspector. 11. The senior Inspector assigns the inspection request to the Inspector. 12. Decision. Has the organization been inspected less than 1 year ago? [Yes: Step 12, No: Step 18]. 13. The inspector contacts the organization representative to confirm if there has been any changes since the last inspection. 14. Decision. Has there been any changes since the last inspection? [Yes: Step 19, No: Step 14] 15. The inspector prepare the inspection report and submits it to the Senior Inspector. This report will specify that no changes has been done since last inspection. The organization complies with the DSC/FSC requirement for the contract. If there is IT requirement for the contract, the inspector will include in the report a recommendation to review the IT requirement. 16. The Senior Inspector will review the inspection report and recommendation. 17. Decision. Is an IT inspection review required? [Yes: Step 17, No: Step 18]. 18. The Senior Inspector assign the IT inspection to an IT inspection specialist. 19. The Inspector make the initial contact with the organization representative via email or phone. The purpose of this first contact is, to introduce himself and describe the inspection process. 20. Decision. Does the organization have to complete a DSC application? [Yes: Step 20, No: Step 31]. The DSC application has to be sent to organization when the inspection will be conducted offsite, or if the contract included IT. 21. The inspector sends the DSC application package to the organization representative (client). A delay of 30 business day is given to the organization to complete and submit this information. 22. Organization has provided information to CSP. 23. Decision. Has client provided the DSC information within the first 10 day of receiving the notice from CSP? [Yes: Step 29, No: 23]. 24. A follow-up notice is sent to the organization representative as a reminder that inspector must receive information to proceed with inspection. 25. Decision. Has client provided the DSC information within the first 20 day of receiving the notice from CSP? [Yes: Step 29, No: 24]. 26. A 2nd follow-up notice is sent to organization representative as a reminder that they must provide the requested information to proceed with inspection. 27. Decision. Has client provided the DSC information within the 25th day of the delay notice? [Yes: Step 29, No: 27].

	28. The Final follow-up notice requesting the completion and submission of the DSC information package is sent to the organization representative. Organization must provide the requested information within the next 5 days. A carbon copy of this notice is sent to the contract authority. 29. Decision. Has client provided the DSC information within the 30 day delay? [Yes: Step 29, No: 45]. 30. Decision. Does the inspector recommend to conduct the inspection onsite instead of offsite? [Yes: Step 30, No: 32] 31. The Senior Inspector approves the inspector's recommendation to conduct an onsite inspection instead. 32. The inspector sends a request for information to the organization representative. The client may or may provide this information before the inspector goes to the organization site to conduct the inspection. The requested information facilitates the preparation for the inspection. 33. The inspector gathers all the information provide for this inspection. 34. The inspector prepares for the inspection. 35. The inspector schedules the inspection. 36. The inspector conduct the inspection. In the case of onsite inspection this step would include the inspector travelling to the organization site to be inspected. 37. The inspector prepares the inspection report. In the case when the organization site does not pass the inspection, the inspector will include in the report, recommendation(s) for the organization. 38. The Senior Inspector reviews the report and makes changes, if required. This may include changes to the recommendation(s). 39. The Manager will review and sign off the report/recommendation(s). 40. Decision. Is Organization Compliant? [Yes: Step 40, No: Step 42] 41. The Inspector sends the notification of compliance to the organization representative and any of the ISS interested parties or at least to the division that triggered the inspection. 42. The inspector closes the inspection request. 43. End of Process 44. The inspector sends a 30 business day notice to the organization representative. The notice will describe the recommendation(s) the organization has to implement at their site in order to comply. They must do so in the delay given. 45. Initiate the Inspection Non-Compliant process. (11 WF CSP Inspection Non-Compliant). 46. Decision. Is the organization compliant? [Yes: Step 40, No: Step 41] 47. The inspector sends a notification to the requestor, which explains that inspection will not be conducted because client failed to send the request information in the 30 business day delay. The inspection request has to be resubmit again. 48. The inspector complete the inspection report in the case that client did not provide the DSC information as requested.
Inputs	• N/A
Outputs	• Report and recommendation • Approval Letter • Letter/notification to inform organization that did not obtaining the DSC clearance requested • Non-compliance Letter

1.1.9 Registration in Contract Security Program – Inspection Non-Compliance

Workflow ID	11 WF CSP Inspection Non-Compliance
Business Unit(s)	• Organization Representative • CSP Inspector
Business Objective	• Conduct physical and information technology security reviews of an organization to assess and ensure: o Organizations are compliant to industrial security requirements. o Information technology security requirements are met. o Level of DSC is appropriate. o Alignment of company and contract information to ensure that all information meets established quality standards. o Provide advice and guidance to CSO's on security requirements.
Trigger	• The inspection process when an organization is sent a 30 day notice to implement recommendations in order for their site to pass the DSC/FSC or IT inspection.
Workflow Description	1. Start Process 2. A notification may be received from the organization representative to inform ISS that the proposed recommendations have been implemented. The dotted line is used to indicate that this event may or may not happen. 3. Decision. Have the recommendations been implemented in the prescribe 30 day delay? [Yes: Step 4, No: Step 7] 4. The Inspector conducts the follow-up inspection. This could be an onsite or offsite inspection. 5. Decision. Did the inspection pass? [Yes: 6, No: 7] 6. End Process. Return to Inspection Workflow. 7. Decision. Was the inspection for a New DCS Site? [Yes: Step 8, No: Step 9]. 8. The inspector prepare and sends the notification that the organization site is not obtaining the DSC clearance as requested. 9. The inspector places the organization into Non-Compliance status. 10. Decision. Is there ongoing contract with this organization at the site in question? [Yes: Step 16, No: Step 11] 11. The inspector gives the organization an additional delay to implement the recommendations. The delay is based on the organization situation and the recommendations that need to be implemented. It can range between 5 to 45 days. 12. Decision. Have the recommendations been implemented in the additional delay? [Yes: Step 13, No: 15]. 13. The Inspector conducts the follow-up inspection. This could be an onsite or offsite inspection. 14. Decision. Did the inspection pass? [Yes: 6, No: 15] 15. The inspector prepare and sends the Non-Compliance notification to the organization and ISS interested parties, particularly the division that triggered the inspection at the start of the process. 16. Initiate the DP 123 process. This is the Compliance and Enforcement with Industrial Security Requirements. 17. End process.
Inputs	• N/A

Outputs	• Letter/notification to inform organization that did not obtaining the DSC clearance requested. • Non-compliance Letter

1.1.10 Registration in Contract Security Program - Investigation

The Organization Investigation business process investigates reported cases of suspected contract security breaches. Investigators gather and review organizational information as well as information regarding the investigation request. If required further investigation is conducted prior to performing the investigation. A report is produced as a result of the investigation which includes recommendations on the best way to handle the security incident. When required other divisions within the CSP, other GC departments or policy authorities are notified of the security incident.

Workflow ID	**12 WF CSP Investigation**
Business Unit(s)	• CSP Inspector (FISO) • CSP Senior Inspector (Senior FISO) • CSP Inspection Manager (FISO Manager) • CISD Director
Business Objective	• Conduct investigations where required.
Trigger	• Various triggers from the other registration workflows.
Workflow Description	1. Start Process. 2. CSP senior inspector performs a preliminary review of the allegation or investigation request. 3. CSP senior inspector determines if the investigation is under the Inspections and Investigations Division (IID) mandate. If the investigation is not under the IID mandate go to step 39. 4. If the investigation is under the IID mandate, the CSP senior inspector performs a risk assessment and prioritizes the investigation request. 5. CSP investigation manager reviews the risk assessment. 6. CSP senior inspector assigns the investigation to an inspector based on the investigations risk and the inspector's experience. 7. CSP inspector gathers additional information and prepares for the investigation. 8. CSP inspector conducts preliminary investigation. 9. CSP inspector determines if the investigation is required. If no investigation is required, go to step 39. 10. If the investigation is required, the CSP inspector will contact the organization's CSO informing of the investigation. 11. CSP Inspector creates and submits to the CSP senior inspector the investigation plan for QA.

	12. Either the CSP senior inspector or CSP inspection manager QA's and approves the investigation plan. 13. If the investigation was not classified as high risk from step 4, go to step 15. 14. If the investigation was classified as high risk from step 4, the investigation plan is submitted to the CSID director for review and approval. 15. The CSP inspector conducts the investigation and determines if there is a "review for cause" for any of the individuals involved in the investigation. If there is "review for cause", the individual is reported to the Security Screening Investigation Unit (SSIU) for a subject interview. The 22 WF CSP SSIU is triggered, otherwise go to step 16. 16. CSP inspector performs analysis of the investigations findings and determines corrective measures. 17. CSP inspector creates a report with corrective recommendations. 18. CSP senior inspector or CSP inspection manager reviews the report and recommendations. 19. The CSP inspection manager determines if there is requirement for a warning letter or if there will be media coverage. If no, go to step 21. 20. If there is a requirement for a warning letter or there will be media coverage, the CISD director reviews the report and recommendations. 21. CSP inspector notifies the other divisions if required. 22. CSP inspector determines if the allegations are confirmed. If the allegations are not confirmed, go to step 37. 23. If the allegations are confirmed, the CSP inspector reports any suspected criminal activity to police authorities. 24. CSP inspector notifies the contract authority and prime contractor. 25. If the report outlined corrective measures, go to step 26. If there were no corrective measures go to step 35. 26. CSP inspector starts the DP 123 process. 27. As a result of the DP 123 process, the CSP inspector determines if there is need for immediate revocation. 28. If there is a need for immediate revocation, the CSP inspector prepares the revocation letter, which is to be sent to the CSO and contract authority. 29. The revocation letter is signed by the director and sent. 30. CSP inspector determines if there is an impact on the organization's employees. If there is no impact, go to step 32. 31. If there is an impact on the organization's employees the SSIU process is triggered (22 WF CSP SSIU). 32. CSP inspector terminates the organization. 33. CSP inspector continues the DP 123 process, go to step 42. 34. If the investigation does not fall under the IID mandate, the CSP senior inspector or CSP inspector will prepare a report. 35. CSP senior inspector or CSP inspector, where required, will notify the other divisions within the Industrial Security Program (ISP) and any other government organizations. 36. If there is a requirement, a follow-up is scheduled. 37. CSP inspector conducts the follow-up. Go to step 42. 38. If no allegations were confirmed, the CSP inspector prepares a report. 39. CSP inspector where required, will notify the other divisions within the Industrial Security Program (ISP) and any other government organizations. Go to step 42. 40. If no corrective measures were required, the CSP inspection manager sends a caution letter to the CSO.

	41. CSO inspection manager requests acknowledgement of the letters receipt. 42. CSP senior inspector closes the investigation. 43. The process ends.
Inputs	• N/A
Outputs	• Investigation results.

1.1.11 Personnel Security Screening Requests

The personnel security screening services business function supports the CSP by providing personnel security screening for CSP registered Canadian private industry employees involved in government contracts with security requirements and other GC department employees when requested. The personnel security screening ensures that the employees working on the secured contracts have the required need to know, trustworthiness and loyalty to Canada at the appropriate security level as outlined by the contract before accessing the protected/classified information, assets or sites. As part of the security screening assessment, the CSP will engage security partners for information regarding the security screening to determine the trustworthiness and loyalty to Canada.

The personnel security requests business process covers the receipt of personnel security request where by the request is verified for completeness and accuracy of information prior to processing. This is achieved by comparing the information within the new request against any existing requests where possible to identify any concerning changes or inconsistencies. Personnel who are unable to provide all the required information for clearance processing are closed out for non-compliance. Personnel security requests are only ever submitted to the CSP by the organizations identified CSO.

Workflow ID	**13 WF CSP PSS Request**
Business Unit(s)	• Organization's Security Official • Individual (Applicant) • CSP Registration • CSP Screening Specialist
Business Objective	• Receipt of and triage of personnel security screening requests.
Trigger	• Organization submission of personnel security screening request. • CSP organization registration. • CSP PSSD created personnel security clearance request.

Workflow Description	1. Start of process. 2. Organization's security official creates a personnel security screening request for an individual employed by the organization. 3. Applicant completes the security screening request. 4. Organization's security officer submits the security screening request. 5. As part of the organization's registration with the CSP, a PSS clearance package is created. 6. The CSP registration PSS package is transferred to the CSP Personnel Security Screening Division (PSSD). 7. In some cases the CSP PSSD have to create personnel security clearance requests. 8. CSP PSSD creates personnel security clearance requests based on external requests received by mail, fax or email. 9. CSP screening specialist reviews if the request is a termination request. If it is a termination request, go to step 29. 10. If the request is not a termination request, the CSP screening specialist reviews the request and verifies the completeness and accuracy of the information. 11. If there are no issues with the request information, go to step 14. 12. If there are issues with the request information, the CSP screening specialist determines if there is a need to request the information from the applicant. If there is a requirement to gather the information, the CSP screening specialist requests the information, go to step 10. 13. If there is no need to request the additional information from the applicant, the CSP screening specialist will close-out the request and return any original documents to the security officials. Go to step 30. 14. If the request received and requires manual input into the PSSD business system, the CSP screening specialist performs the data entry. 15. Depending on the nature of the request, one of the following sub processes will be triggered. If the request is for a new personnel security clearance, the new sub process is triggered. 16. The new personnel security process is triggered. (14 WF CSP PSS New). 17. If the request is an update to an existing clearance. 18. The update personnel security process is triggered. (15 WF CSP PSS Update). 19. If the request is an upgrade to an existing clearance. 20. The upgrade personnel security process is triggered. (16 WF CSP PSS Upgrade). 21. If the request is to transfer a clearance from one organization to another. 22. The transfer personnel security process is triggered. (17 WF CSP PSS Transfer). 23. If the request is to duplicate an existing clearance. 24. The duplicate personnel security process is triggered. (18 WF CSP PSS Duplicate). 25. If the request is a reactivate a clearance. 26. The reactivation personnel security process is triggered. (19 WF CSP PSS Re-Activation). 27. If the request is for a NATO/COSMIC clearance. 28. The NATO/COSMIC personnel security process is triggered. (21 WF CSP NATO). 29. The termination process is triggered (20 WF CSP PSS Terminate). 30. End Process.

Inputs	• Personnel Security Clearance Requests
Outputs	• Close-out of security clearance request. • Triggering of any of the various PSSD processes.

1.1.12 Personnel Security Screening - New

The personnel security screening business process evaluates the personnel based on the security level specified in the contracts security requirements. The personnel security screening evaluates the personnel's need to know, background information, criminal records checks, out of country checks, fingerprint checks, credit checks, Law Enforcement Record Check (LERC), open source inquiries, CSIS background check and polygraph checks depending on the requested security level. Personnel who are deemed to be trustworthy and loyal to Canada are granted one of the following personnel security clearance types:

a. Reliability Status;
b. Site Access Status;
c. Reliability Enhanced Status;
d. Secret Clearance;
e. NATO/COSMIC;
f. Site Access Clearance;
g. Top Secret Clearance;
h. Top Secret SIGNIT Clearance; or
i. Top Secret Enhanced Clearance.

Personnel found in good standing are granted the requested security clearance and can now work on GC protected/classified information and assets. Personnel that are unable to be meet the clearance analysis are further processed by the Security Screening Investigation Unit for a resolution of doubt. At which point, the personnel will be granted the requested security clearance or closed out for non-compliance.

Site Access is required when personnel require temporary access to sensitive GC related sites or facilities but not to any information/assets.

Personnel security clearances which involve the exchange of information/assets with countries participating in NATO require a special NATO briefing and NATO certificate. All Canadian citizens are eligible for Canadian granted NATO clearances, however, NATO clearances for citizens of other NATO countries must be granted by that country.

Workflow ID	14 WF CSP PSS New
Business Unit(s)	• CSP Screening Specialist
Business Objective	• Processing of new personnel security clearance requests.
Trigger	• New personnel security clearance requirement.
Workflow Description	1. Start of process. 2. For reliability and site access status requests, PSS screening specialist will trigger the following security checks, Fingerprint Document Control Number (DCN) matching, where the request's DCN is matched to a set of fingerprint results from the RCMP. 3. PSS screening specialist will perform a Credit Check of the individual. 4. PSS screening specialist will determine if an Out of Country Verification (OCC) is required. If no OCC is required, go to step 6. 5. If an OCC is required, an OCC is performed. 6. PSS screening specialist analyzes the results from the fingerprints, credit and OCC checks. 7. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 11. 8. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 11. 9. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 10. If no additional processing is required, go to step 50. 11. If the request requires reliability enhanced status, continue, otherwise go to step 20. 12. For reliability enhanced status, the PSS screening specialist will trigger the following security checks, Law Enforcement Record Check (LERC). 13. PSS screening specialist will request that the individual completed a security questionnaire or partake in a security interview. 14. PSS screening specialist will perform an open source inquiry of the individual. 15. PSS screening specialist analyzes the results from the LERC, security questionnaire/interview and open source inquiry. 16. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 20. 17. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 20. 18. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 19. If no additional processing is required, go to step 50. 20. If the request requires secret and site access clearance, continue, otherwise go to step 27. 21. For secret and site access clearance, the PSS screening specialist will trigger a CSIS security assessment. 22. PSS screening specialist analyzes the results from the CSIS security assessment.

	23. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 27. 24. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 27. 25. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 26. If no additional processing is required, go to step 50. 27. If the request requires a top secret clearance, continue, otherwise go to step 34. 28. For a top secret clearance, the PSS screening specialist will trigger a CSIS security assessment. 29. PSS screening specialist analyzes the results from the CSIS security assessment. 30. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 34. 31. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 34. 32. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 33. If no additional processing is required, go to step 50. 34. If the request requires a top secret SIGNIT clearance, continue, otherwise go to step 39. 35. For top secret SIGNIT clearance, the PSS screening specialist will trigger an additional credit check. 36. The PSS screening specialist will then trigger a SSIU subject interview. 37. The SSIU process is triggered (22 WF CSP PSS SSIU). 38. If no additional processing is required, go to step 50. 39. If the top secret enhance clearance is required, continue, otherwise go to step 48. 40. For top secret enhance clearance, the PSS screening specialist will trigger a security questionnaire or interview. 41. PSS screening specialist will perform an open source inquiry. 42. PSS screening specialist will request a CSIS security assessment. 43. PSS screening specialist will request the individual undergo a polygraph examination. 44. PSS screening specialist analyzes the results from the security questionnaire/interview, open source inquiry, CSIS security assessment and polygraph results. 45. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 48. 46. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 48. 47. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). Go to step 50. 48. PSS screening specialist performs a completeness verification on the personnel security request. 49. PSS screening specialist creates the briefing certificate and sends it to the organizations CSO. 50. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Personnel Security Clearance Request • Results from the various security checks (credit checks, CSIS security assessment, etc.)
Outputs	• Granting of personnel security clearance request • Briefing certificate

1.1.13 Personnel Security Screening - Update

The Personnel Security Screening Update business process involves the submission of information for the purpose of renewal or simple update. Renewal requests are treated the same as new personnel security requests, whereas updates require the received information to be reviewed and analyzed to ensure completeness. Based on the nature of the update it is possible that this business process could require additional back ground checks which could impact the already granted security clearance. In the situation where the update processes normally a new security clearance briefing is issued. Failure to provide required information results in the close out of the personnel security clearance for non-compliance.

Workflow ID	**15 WF CSP PSS Update**
Business Unit(s)	CSP screening specialist
Business Objective	To update an existing PSSD security clearance.
Trigger	Update to personnel security clearance requirement.
Workflow Description	1. Start of process. 2. CSP security specialist determines the type of update being performed. If it is an actual update to the existing information, go to step 4. 3. If the update is a renewal, trigger the new security clearance process (14 WF CSP PSS New) as it has the same requirements and actions. Go to step 15. 4. CSP security specialist determines if all the information is received in the request. If all the information has been received, go to step 7. 5. CSP security specialist determines if there is a need to request additional information from the organization's CSO. If there is a need to request additional information, go to step 4. 6. If there is no requirement to request additional information, the CSP security specialist will close-out the request and return any original documentation to the CSO. 7. CSP security specialist will update the individual's information based on the provided information. 8. CSP security specialist will note if there was a change in the individual's personal circumstances. If there was a change in personal circumstance, go to step 10. 9. If there was no change in personal circumstance, the CSP security specialist notifies CSIS. 10. CSP security specialist will contact CSIS with the new information and request a new CSIS security assessment. 11. CSP security specialist analyzes the results of the CSIS security assessment. If there were no adverse results, go to step 13. 12. If the CSIS security assessment produced adverse results the SSIU process (22 WF CSP PSS SSIU) is triggered. Go to step 15. 13. CSP security specialist performs a completeness verification on the request.

	14. CSP security specialist issues a new briefing certificate and sends it to the organization's CSO. 15. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Personnel Security Clearance Request • Results from the CSIS security check
Outputs	• Briefing certificate

1.1.14 Personnel Security Screening - Upgrade

The personnel security screening upgrade business process involves the upgrade a of personnel security clearance from one level to another. The received request is assessed to determine if the previous security clearance checks need to be redone. After which it is determined if the upgrade needs to continue or not. If the upgrade needs to continue, then the security checks are performed for the desired clearance level. At any point during the personnel security upgrade process if there are any adverse results, the SSIU business process would be triggered for a resolution of doubt. In the event that the personnel security upgrade is successful a new security clearance would be granted and briefing certificate provided to the organization.

Workflow ID	**16 WF CSP PSS Upgrade**
Business Unit(s)	• CSP Screening Specialist
Business Objective	• Processing of an upgrade to existing personnel security clearance requests.
Trigger	• Upgrade personnel security clearance requirement.
Workflow Description	1. Start of process. 2. If the request is to upgrade to a reliability enhanced status, continue, otherwise go to step 16. 3. PSS screening specialist will assess the request to determine if the reliability security checks need to be redone. 4. If there is no need to redo the reliability security checks, go to step 8. 5. PSS screening specialist analyzes the results from the reliability security checks. If there were no adverse results, go to step 7. 6. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU). 7. If no additional processing is required, go to step 66.

	8. If additional processing is required, the PSS screening specialist will trigger the following security checks, Law Enforcement Record Check (LERC). 9. PSS screening specialist will request that the individual completed a security questionnaire or partake in a security interview. 10. PSS screening specialist will perform an open source inquiry of the individual. 11. PSS screening specialist analyzes the results from the LERC, security questionnaire/interview and open source inquiry. 12. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 15. 13. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 15. 14. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 15. If no additional processing is required, go to step 64. 16. If the request is to upgrade to secret and site access clearance, continue, otherwise go to step 28. 17. PSS screening specialist will assess the request to determine if the secret security checks need to be redone. 18. If there is no need to redo the secret security checks, go to step 22. 19. PSS screening specialist analyzes the results from the secret security checks. If there were no adverse results, go to step 21. 20. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU). 21. If no additional processing is required, go to step 66. 22. For secret and site access clearance, the PSS screening specialist will trigger a CSIS security assessment. 23. PSS screening specialist analyzes the results from the CSIS security assessment. 24. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 27. 25. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 27. 26. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 27. If no additional processing is required, go to step 64. 28. If the request is to upgrade to top secret clearance, continue, otherwise go to step 40. 29. PSS screening specialist will assess the request to determine if the top secret security checks need to be redone. 30. If there is no need to redo the top secret security checks, go to step 34. 31. PSS screening specialist analyzes the results from the top secret security checks. If there were no adverse results, go to step 33. 32. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU). 33. If no additional processing is required, go to step 66. 34. For a top secret clearance, the PSS screening specialist will trigger a CSIS security assessment. 35. PSS screening specialist analyzes the results from the CSIS security assessment. 36. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 39. 37. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 39. 38. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). 39. If no additional processing is required, go to step 64.

	40. If the request is to upgrade to top secret SIGNIT clearance, continue, otherwise go to step 41. 41. PSS screening specialist will assess the request to determine if the top secret SIGNIT security checks need to be redone. 42. If there is no need to redo the top secret SIGNIT security checks, go to step 46. 43. PSS screening specialist analyzes the results from the top secret SIGNIT security checks. If there were no adverse results, go to step 45. 44. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU). 45. If no additional processing is required, go to step 66. 46. For top secret SIGNIT clearance, the PSS screening specialist will trigger an additional credit check. 47. The PSS screening specialist will then trigger a SSIU subject interview. 48. The SSIU process is triggered (22 WF CSP PSS SSIU). 49. If no additional processing is required, go to step 64. 50. The request is to upgrade to top secret enhanced clearance. 51. PSS screening specialist will assess the request to determine if the top secret security checks need to be redone. 52. If there is no need to redo the top secret security checks, go to step 56. 53. PSS screening specialist analyzes the results from the top secret security checks. If there were no adverse results, go to step 55. 54. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU). 55. If no additional processing is required, go to step 66. 56. For top secret enhance clearance, the PSS screening specialist will trigger a security questionnaire or interview. 57. PSS screening specialist will perform an open source inquiry. 58. PSS screening specialist will request a CSIS security assessment. 59. PSS screening specialist will request the individual undergo a polygraph examination. 60. PSS screening specialist analyzes the results from the security questionnaire/interview, open source inquiry, CSIS security assessment and polygraph results. 61. PSS screening specialist determines if there are any adverse results that could impact the granting of the clearance. If there are no adverse results, go to step 64. 62. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 64. 63. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). Go to step 66. 64. PSS screening specialist performs a completeness verification on the personnel security request. 65. PSS screening specialist creates the briefing certificate and sends it to the organizations CSO. 66. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Personnel Security Clearance Request • Results from the various security checks (credit checks, CSIS security assessment, etc.)
Outputs	• Granting of personnel security clearance request • Briefing certificate

1.1.15 Personnel Security Screening - Transfer

The Personnel Security Clearance Transfer business process involves the transfer of a CSP personnel security clearance from either an outside organization into the CSP or from the CSP out to an Other Government Department (OGD). In both cases the current personnel security request is verified to be valid and if a renewal is required prior to transfer. In the cases where the current security clearance is no longer valid, the request is closed and the organization is notified to submit a new one. Security clearances that require a renewal are simply transferred with a note on file to the receiving OGD.

Personnel Security Clearance Transfer to the CSP, where the requested status is higher than the current security clearance level, the organization is informed to submit an upgrade security clearance request and the transfer occurs at level. The transferred security clearance is then assessed to determine if any security checks need to be redone. In the case there is adverse results from the security checks, the SSIU business process is evoked for a resolution of doubt. Otherwise, a new security clearance briefing certificate would be granted and provided to the organization.

Workflow ID	**17 WF CSP PSS Transfer**
Business Unit(s)	• CSP Screening Specialist
Business Objective	• To process the transfer of an existing personnel security screening request
Trigger	• Transfer personnel security screening requirement.
Workflow Description	1. Start of process. 2. If the clearance is being requested by another government department (OGD) to be transferred from PWGSC, continue, if PWGSC is requesting the transfer, go to step 9. 3. Verify that the existing clearance is still active. 4. If the clearance is not valid, continue, otherwise go to step 7. 5. Notify the OGD of invalid clearance and inability to transfer file 6. Close out request, go to step 23. 7. If the clearance requires no renewal, continue, otherwise go to step 9 8. Attach a note on the file to the OGD stating a renewal is required. 9. Send a copy of clearance to the requesting OGD. 10. Notify CSIS of the transfer of the request, go to step 23. 11. If OGD states the clearance is not valid, continue, otherwise go to step 14 12. Close out transfer request. 13. Notify CSO of the new to submit a new request as the transfer request cannot be completed. Go to step 23. 14. If the clearance or status level held is at a lower level than requested, continue, otherwise go to step 17.

	15. Inform CSO that an upgrade request is required to be given the clearance level requested. 16. Continue with the transfer at the level of applicant's clearance/status. 17. Assess the request to determine if security checks need to be redone. 18. If security checks must be redone, continue, otherwise go to step 21. 19. If adverse results are found when redoing security checks, continue, otherwise go to step 21. 20. Trigger the SSIU process (22 WF CSP PSS SSIU). 21. Verify completeness of the request. 22. Create a briefing certificate for the request and send it to the CSO. 23. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Personnel Security Clearance Transfer request
Outputs	• Transfer of completed security clearance/status

1.1.16 Personnel Security Screening - Duplication

The personnel security clearance duplication business process involves the duplication of a personnel security clearance where individuals are employed by multiple registered organizations. Security clearances are validated and the request is closed out and the organization is notified to submit a new request. The personnel security clearance to be duplicated is then evaluated to determine if any of the previous security checks need to be redone. Adverse results from the security checks triggers the SSIU process for a resolution of doubt, otherwise a new security clearance briefing certificate would be granted and provided to the organization.

Workflow ID	**18 WF CSP PSS Duplicate**
Business Unit(s)	• CSP Screening Specialist
Business Objective	• To process the duplication of an existing personnel security screening request
Trigger	• Duplication personnel security screening requirement

Workflow Description	1. Start of process. 2. If no valid personnel security clearance exists at the level requested, continue, otherwise go to step 5. 3. Close out request. 4. Notify CSO of the need to submit a new screening request as the previous level requested cannot be duplicated. Go to step 11. 5. Assess the previous request to determine if additional security checks need to be redone. 6. If security checks must be redone, continue, otherwise go to step 9. 7. If adverse results are found when redoing security checks, continue, otherwise go to step 9. 8. Trigger the SSIU process (22 WF CSP PSS SSIU). 9. Verify completeness of the request. 10. Create a briefing certificate for the request and send it to the CSO. 11. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Personnel Security Clearance request (Duplication)
Outputs	• Briefing Certificate

1.1.17 Personnel Security Screening - Reactivation

The personnel security clearance reactivation business process reviews how long ago a personnel security clearance request was terminated and if it is necessary to redo the clearance's security checks. Adverse results from the security checks results in the triggering of the SSIU process for a resolution of doubt determination. Otherwise, the terminated security clearance is duplicated and then reactivated. A new security clearance briefing is granted and provided to the organization.

Workflow ID	**19 WF CSP PSS Re-activation**
Business Unit(s)	• CSP Screening Specialist
Business Objective	• To process the reactivation of an existing personnel security screening request
Trigger	• Organization reactivation requirement.

Workflow Description	1. Start of process. 2. If the clearance to be re-activated has been terminated for over 2 years, continue, otherwise go to step 5. 3. Close out re-activation request. 4. Notify CSO of the need to submit a new screening request. Go to step 14. 5. If the clearance to be re-activated has been terminated between 1 and 2 years, continue, otherwise go to step 9. 6. Redo necessary security checks. 7. If adverse results are found when redoing security checks, continue, otherwise go to step 11. 8. Trigger the SSIU process (22 WF CSP PSS SSIU). 9. If the clearance to be reactivated has not been terminated yet, continue, if it has been terminated less than 1 year, go to step 11. 10. No termination has ever been received and the initial request is still active 11. Duplicate the clearance request. 12. Verify completeness of the request. 13. Create a briefing certificate for the request and send it to the CSO. 14. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Personnel Security Clearance Request (Re-activation)
Outputs	• Briefing Certificate

1.1.18 Personnel Security Screening - Termination

The personnel security clearance termination business process ensures that all required information is received for the termination request, otherwise the request is closed out. Should there be any pending CSIS request, CSIS is notified then the security clearance termination is processed.

Workflow ID	**20 WF CSP PSS Termination**
Business Unit(s)	• Organization's Security Official • Personnel Screening Specialist
Business Objective	• To terminate a personnel security clearance.
Trigger	• Personnel screening termination requirement.

Workflow Description	1. Start of process. 2. Organization's Security Official submits a request to terminate a PSS request. If the request is submitted through OLISS, go to step 6. 3. If the CSO submits a manual request to terminate a PSS, the screening specialist reviews the information and verifies if the CSO's signature is on the termination request. If there are no issues with the request, go to step 7. 4. If the signature is not on the termination request, the screening specialist requests a signed termination form from the CSO. 5. If the information is not received, the screening specialist will close-out the request. 6. If the CSO submits an OLISS request to terminate a PSS, the request is matched to the existing Personnel ID. 7. The screening specialist will verify if there is a pending PSS request with the same Personnel ID (for the same organization) at CSIS. If there is no pending request with CSIS, go to step 9. 8. If a PSS request for the same organization is still pending with CSIS, the screening specialist will notify CSIS of the termination request. 9. The screening specialist terminates the PSS request. 10. The PSS request is set to "Struck off Strength". 11. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• Termination Request
Outputs	• Personnel Security Clearance Termination

1.1.19 Personnel Security Screening - NATO Requests

The personnel security clearance NATO process ensures that all required information is received for NATO briefings and NATO certificates for Personnel security clearances which involve the exchange of information/assets with countries participating in NATO. If the individual satisfies the criteria and the CSO sends the required information to IISD, the NATO request will be issued.

Workflow ID	**21 WF CSP NATO Requests**
Business Unit(s)	• Organization's Security Official • NATO Partner • Personnel Screening Specialist
Business Objective	• To issue NATO briefings and NATO certificates for Personnel Security Clearances
Trigger	• NATO clearance request.

Workflow Description	1. Start of process. 2. CSO submits a NATO clearance request. 3. NATO request initiated by PSSD. 4. The screening specialist verifies if there is an existing and valid clearance for the individual (including DC Pending NATO requests). 5. If there is no valid clearance, the screening specialist will initiate a security clearance request. 6. The screening specialist will identify the type/level of security clearance required and follow the PSSD process. 7. If there is a valid clearance, the screening specialist will assign the NATO request to the Pending NATO Workflow for IISD to action. 8. The IISD analyst will first verify if a National Clearance is granted. If a clearance has not been granted, return to step 5. 9. If the National Clearance is granted, the IISD analyst will verify if the individual is a Canadian Citizen. 10. If the individual is a Canadian Citizen, the IISD analyst will determine if the NATO FSC meets or exceed the requirements level. 11. If the individual is not a Canadian Citizen, the ISSD analyst will verify if the individual is a NATO National. 12. If the NATO FSC meets or exceeds the requirements level and the individual is a NATO National with more than 5 years of Canadian residency, go to step 19. If the NATO FSC does not meet the requirements level, go to step 13. 13. The IISD Analyst performs the Personnel Security Clearance Information sheet process. 14. If the individual is a Canadian Citizen and a Non NATO National (NNN), the IISD analyst will determine if the individual will require a NATO Office of Security, Security Assessment (NNN/NOS SA). If not, go to step 17. 15. If the individual does require a NNN/NOS SA, the IISD analyst will verify if the DSA's NNN approval is indicated in sections 42/42/44. If the approval is not valid, go to step 17. 16. If the approval is valid, the IISD analyst will complete the NATO letter process. 17. The IISD analyst will inform the organization of the assessment results. 18. The IISD analyst will send a briefing form to the CSO for signature. 19. The CSO must return the signed briefing form to IISD within 10 working days. 20. If the signed briefing form is not received by IISD within 10 working days, the IISD analyst will request the signed form from the CSO. If the briefing form is not received, go to step 26 21. The signed briefing form is received by IISD within 10 working days. 22. The IISD analyst reviews the signed briefing form. 23. The IISD analyst will match the NATO expiry date to the National Clearance expiry date. 24. The IISD Analyst will determine if the NATO request is granted or denied. 25. If the signed briefing form was not received for the NATO request or the request is denied by the IISD analyst, the NATO request is closed out. 26. If all the required information is received for the NATO request, the IISD analyst provides the information to the foreign partner, the CSO and the individual. 27. Return to the PSS Requests process to end (13 WF CSP PSS Request).
Inputs	• NATO Request

Outputs	• NATO briefings and NATO certificates for Personnel security clearances

1.1.20 Personnel Security Screening - Investigations

The Personnel Security Screening Investigations business process is to obtain additional information from the applicant. An interview is required to assess eligibility for a security clearance. It may review elements such as character, financial situation, time spent out of country, and personal beliefs and associations. It is based on an evaluation of the results of security assessments such as Criminal Records Name Checks, reliability checks, and loyalty. An interview can all be triggered as a result of an organization inspection or investigation if there was a security incident. Similarly, an organization inspection or investigation can be initiated as a result of Subject Interview.

A Subject Interview is conducted in order to determine the nature of the circumstances or activity which caused a security concern during the screening process. It also gives the individual an opportunity to provide specific information to respond to these concerns. Subject Interviews are mandatory for Top Secret SIGINT security clearances. The CSP will inform the individual and their organization of the results by registered letter.

Workflow ID	**22 WF CSP SSIU**
Business Unit(s)	• Inspections/Investigations Division • Personnel Screening Specialist • Security Screening Investigation Unit (SSIU) Team • CISD Director • PWGSC Legal Team • PWGSC Deputy Minister
Business Objective	• To investigate and determine the eligibility of a Personnel Security Clearance.
Trigger	• Personnel Screening Request transferred to SSIU for further investigation.
Workflow Description	1. Start of process. 2. Inspections/Investigations Division submits a request or provides information to SSIU (10 WF CSP Inspections or 12 WF CSP Investigations). 3. PSSD receives a request requiring an SSIU investigation. 4. PSSD submits a request or provides information to SSIU. 5. The SSIU Liaison Officer reviews the file for completeness and confirms the checks performed.

	6. If the file is missing information, go to step 4. 7. If the file is not missing any information and the checks have been verified, a CSIS assessment must be completed when required. 8. The SSUI Liaison Officer transfers the file to the SSIU Chief for triage. 9. The SSIU Chief will determine if the PSS will be suspended. 10. The SSIU Chief determines the PSS is to be suspended based on the security request type of the file. 11. If the security request is at the classified level, the file will be sent to the Deputy Minister for suspension approval. 12. If the security request is at the reliability level, the file will be sent to the CISD Director for suspension approval. 13. If the SSIU Chief determines that there is no requirement for a suspension, the Chief will determine if an SSIU investigation is required. If it is not required, go to step 28. 14. If an SSIU investigation is required, the SSIU Chief assigns the file to an SSIU Officer for action. 15. The SSIU Officer prepares for a resolution of doubt interview with the individual. 16. The SSIU Officer conducts a resolution of doubt interview with the individual. 17. Following the interview, the SSIU Officer will verify and validate the resolution of doubt interview results. 18. The SSIU Officer will complete an SSIU report and propose a recommendation for the file. 19. If the recommendation from the SSIU Officer is a denial of the PSS, a denial package is prepared by the officer. 20. The SSIU officer must determine if a follow-up interview is required with the individual. 21. If a follow-up interview is required, the SSIU Officer will schedule an interview with the individual. 22. If a follow-up interview is not required, the SSIU Officer will submit a report with the recommendation for review by the SSIU Chief. 23. The SSIU Chief will review the report and recommendation. 24. The SSIU Chief will determine if a follow-up interview is required with the individual. If a follow-up is required, go to step 21. 25. If a follow-up interview is not required, the SSIU Chief will determine is modifications are required for the report and recommendation proposed. 26. If the SSIU chief determines modifications are required, the SSIU Officer will update the report and recommendation. Once updated, go to step 22. 27. If the SSIU chief determines that no modifications are required, the SSIU Chief will assign the file to the SSIU Liaison Officer for action based on the recommendation outlined in the report. 28. If the recommendation is to grant the PSS request, go to step 29. 29. The SSIU Liaison Officer grants the PSS request. 30. The SSIU Liaison Officer verifies if any additional processing is required. If there is no additional processing required, go to step 50. 31. If the SSIU Liaison Officer determines there is additional processing required, the file is transferred to the appropriate PSS workflow for action by PSSD. 32. If the recommendation is to close out the PSS request, go to step 33. 33. The SSIU Liaison Officer creates the close out letter and sends it to the CSO. Once sent, go to step 50.

	34. If the recommendation is to terminate the PSS request, go to step 35. 35. The SSIU Liaison Officer informs the CSO that a termination request must be sent to PSSD for action. Once the CSO is informed, go to step 50. 36. If the recommendation is to deny or revoke the PSS request, go to step 37. 37. The report and denial letter is reviewed by the legal team. 38. If the legal team determines that no modifications are required for the report and/or the denial letter, go to step 40. 39. The SSIU Chief must update the report and denial letter proposed by the legal team. Once completed, go to step 37. 40. The report and denial letter will be reviewed once again by the legal team for final approval. 41. If the security request type of the file is at the reliability level, the CISD director must review the report and denial letter. If no modifications are proposed by the CISD director, go to step 44. 42. If the CISD director determines that modifications are required for the report and/or denial letter, go to step 43. 43. The SSIU Chief must update the report and denial letter based on the modifications proposed by the CISD director. Once completed, go to step 41. 44. The CISD director will approve or deny the recommendation. If the CISD Director approves the denial, go to step 49. If the CISD Director does not approve the denial, the next step of the process is still being developed and is unknown at this point. 45. If the security request type of the file is at the classified level, the Deputy Minister must review the report and denial letter. 46. If the Deputy Minister determines that modifications are required for the report and/or denial letter, go to step 47. 47. The file is returned to the SSIU Chief to update the report and denial letter based on the modifications proposed by the Deputy Minister. 48. If the Deputy Minister approves the report and denial letter, go to step 49. If the Deputy Minister does not approve the report and denial letter at this stage of the process, the next step is still being developed and is unknown at this point. 49. The SSIU Liaison Officer will send a notification to the CSO, the Individual and CSIS of the decision. 50. The process ends.
Inputs	• Eligibility of Personnel security clearances
Outputs	• Issuance or Revocation of Personnel security clearances

1.1.21 Call Centre

The ISP Call Centre fields inquiries from the various CSP and CGP clients. In the situation where possible, the Call Centre will provide the response, otherwise the inquiry is assessed and assigned to the appropriate CSP or CGP business line for response/action.

Workflow ID	23 WF CSP Call Centre
Business Unit(s)	• External Contact (Contract Security Officer, Designated Official, etc.) • Call Centre Analyst • Call Centre Senior Analyst • ISP Business Line (CSP or CGP)
Business Objective	• Outline of the Call Centre activities from received request to supplied response.
Trigger	• Client inquiry with the ISS.
Workflow Description	1. Start of process. 2. External to ISP client submits an inquiry request to the Call Centre. The inquiry can be in the form of a phone call, left voicemail or email. 3. Call Center Analyst determines if the information can be disclosed to the individual making the inquiry. If the information cannot be disclosed, the individual is notified, proceed to step 17, otherwise continue to step 4. 4. Call Center Analyst analyzes the inquiry to determine if it a Tier 1 request. A Tier 1 request is any request where the response can easily be obtained with existing tools and the response can be immediately provided. If the inquiry is determined to be Tier 1, go to step 13. If not Tier 1, go to step 5. 5. Call Center Analyst determines if the inquiry is of type Tier 2. A Tier 2 request is any request where the response requires a level of interpretation or judgement with a detailed response. If the inquiry is determined to be Tier 2, go to step 7. If not Tier 2, go to step 6. 6. The inquiry is of type Tier 3, which requires a response from the responsible ISP business line (CSP or CGP). Proceed to step 8. 7. Call Center Analyst determines if the Tier 2 request requires Call Center Senior Analyst assistance. If no assistance is required, go to step 13, otherwise continue to step 8. 8. Call Center Senior Analyst determines if triage of the inquiry is required. If triage is not required go to step 11, otherwise continue to step 9. 9. Call Center Senior Analyst triages the inquiry to determine which ISP business line to transfer the request to. 10. Call Center Senior Analyst sends the inquiry to the ISP business line for response. Continue at step 12. 11. Call Center Senior Analyst in conjunction with the Call Center Analyst develops the inquiry response. Go to step 14. 12. The ISP business line develops the inquiry response. Continue to step 14. On occasion the ISP business will provide the response directly back to the client, in this case go to step 16. 13. Call Center Analyst develops the inquiry response. 14. Call Center Analyst provides the inquiry response to the client. 15. Call Center Analyst logs the call within the business system DISIS for tracking purposes. 16. The ISP business line provides the inquiry response to the client.

	17. The process ends.
Inputs	• Client inquiry.
Outputs	• Response to client inquiry.

1.1.22 CSP Visits

The CSP processes both international and domestic secured site visit requests. As the Canadian designated security authority, the CSP ensures the safeguarding of national security by making sure required contract security requirements are adhered to, preventing unauthorized access to sensitive information and assets.

Workflow ID	**24 WF CSP Visits**
Business Unit(s)	• Security Officials • CSP Visit Officers
Business Objective	• To process visit request to Canada and from Canada and ensure that security requirements are maintained.
Trigger	• Need for Canadian industry or Canadian Government to visit other Canadian, United States or Foreign sites. Likewise, if there is a need for United States or Foreign entities to visit a Canadian industry or Canadian government site.
Workflow Description	1. Start of process 2. Security Official submits a Request for Visit (RFV) to the CSP. The RFV can be for one of several visit types and are generally submitted by: a. Canada to Canada, Canada to United States and Canada to Foreign visit requests are received via email. b. United States to Canada visits are received via the United States Department of Defence's Defence Security Service (DSS), which is received by DND and relayed to the CSP via an email from DND's Director Foreign Liaison (DFL3) system. c. Foreign to Canada visits are received via DND's Director Foreign Liaison (DFL3) system and relayed to the CSP via an email. They can also be received in a direct email from foreign entity to the CSP. 3. CSP Visit Officer reviews the RFV. 4. CSP Visit Officer validates the security requirements of the visit. This is done by reviewing the referenced contract, the organization's clearance level and status as well as all individual security clearances as required. In the case of foreign visits

	to or from Canada, the country is requested to validate the organization and individual clearance levels and to provide assurance. 5. CSP Visit Officer determines if the RFV is complete. If it is complete go to step 9, 14, 15, 18 or 19 depending on the type of visit, otherwise continue to step 6. 6. CSP Visit Officer determines if the RFV should be rejected or not. If it is determined that the RFV is to be rejected go to step 25, otherwise continue to step 7. 7. CSP Visit Officer sends a request to the RFV security officer for missing information. 8. Security Official provides the required information. Go to step 3. 9. RFV type is a Canada to Canada visit. 10. Canada to Canada visit is either of subtype Industry or DND. If DND go to step 13, otherwise go to step 11. 11. CSP Visit Officer requests host site concurrence for the visit. 12. CSP Visit Officer receives host site response for concurrence. Go to step 24. 13. CSP Visit Officer sends the RFV to DND. Go to step 24. 14. DND approves the RFV and notifies the CSP. Go to step 24. 15. RFV type is a United States to Canada visit. Go to step 17. 16. RFV type is a Foreign to Canada visit. 17. CSP Visit Officer requests host site concurrence for the visit. 18. CSP Visit Officer receives host site response for concurrence. Go to step 24. 19. RFV type is Canada to Foreign visit. Go to step 21. 20. RFV type is Canada to United States visit. 21. CSP Visit Officer requests foreign DSO concurrence. 22. CSP Visit Officer received foreign DSO concurrence. 23. CSP Visit Officer determines if the RFV is to be approved. If the RFV is not approved go to step 25, otherwise go to step 24. 24. CSP Visit Officer creates the RFV approval notice. Go to step 26. 25. CSP Visit Officer creates the RFV rejection notice. 26. CSP Visit Officer sends the notification to the security official who submitted the RFV and the visit's host site. 27. The process ends.
Inputs	• Request for Visit • Contract security clauses • Host site concurrence
Outputs	• Request for visit approval or rejection • Approval or rejection notification

1.2 CONTROLLED GOODS PROGRAM PROCESSES

1.2.1 Registration in Controlled Goods Program - New

Workflow ID	25 WF CGP Registration New
Business Unit(s)	• Registering Organization (Applicant) • CGP Program Support Clerk • CGP Program Support Information Officer • CGP Registration Coordinator • CGP Registration Chief • CGP Registration Analyst • CGP Operations Manager • CGP Case Management and Best Practices (CMBP) • CGP Investigations and Analysis Unit (IAU) • CGP Program Management and Learning (PML) • CGP Compliance
Business Objective	• To register a new organization with the ISS Controlled Goods Program (CGP).
Trigger	• Organization requirement to register with the ISS CGP due to being in possession or having access to controlled goods.
Workflow Description	1. Start of process. 2. Applicant completes and submits the CGP registration application. 3. CGP program support clerk reviews the registration application. 4. CGP program support clerk determine if all required information has been received. If all information received, go to step 7. 5. If there is missing information, CGP program support clerk requests missing information from applicant. 6. Applicant provides requested information, go to step 2. 7. CGP program support clerk performs preliminary data entry. 8. CGP program support information officer validates the application. 9. CGP program support information officer determines if all required information has been received. If all information has been received, go to step 14. 10. CGP program support information officer determines if the application is to be rejected based on the incomplete application. If the application is rejected, go to step 13.

	11. If the application is not being rejected, the CGP program support information officer requests the missing information from the applicant. 12. Applicant provides the missing information. Go to step 8. 13. If the application is being rejected from step 10, CGP program support information officer notifies the applicant of the application rejection. Go to step 48. 14. If all the information was received, CGP program support clerk completes the data entry of the application. 15. CGP program support information performs a QC of the inputted data. 16. CGP program support information reviews the applicant's security assessment (SAA) as part of the application. 17. CGP program support information notifies the applicant that the CGP registration is in process. 18. CGP program support information requests security checks (Fingerprints, Criminal Record Name Check, Credit Check, etc.) as required. 19. CGP program support information notifies PML if an organization's Designated Official (DO) requires training. 20. CGP training process is triggered. (28 WF CGP Designated Official Training). 21. CGP registration coordinator triages and assigns the registration application to a CGP registration analyst for processing. 22. CGP registration analyst reviews the application and SAA for completeness. 23. CGP registration analyst determines if all required information has been received. If all the required information has been received, go to step 26. 24. CGP registration analyst requests the missing information from the applicant. 25. Applicant provides the missing information. Go to step 22. 26. CGP registration analyst completes the registration data entry. 27. CGP registration analyst analyzes the application and SAA. 28. CGP registration analyst determines if a referral to CGP investigations and analysis unit (IAU) is required. If no referral is required, go to step 30. 29. If a CGP IAU referral is required, the CGP IAU process is triggered. (29 WF CGP Investigations and Analysis (IAU)). Go to step 32. 30. CGP registration analyst determines if a referral to CGP Case Management and Best Practices (CMBP) is required. If a CGP CMBP referral is not required, go to step 32. 31. If a CGP CMBP referral is required, the CGP CMBP process is triggered (34 WF CGP CMBP). Go to step 32. 32. CGP registration analyst receives all the results from the previous steps and determines if the CGP registration application is to be approved, rejected or if the case is high risk. If the CGP registration application is being rejected, go to step 35. If the CGP registration application is being approved, go to step 38. 33. If the CGP registration application is considered to be high risk, the CGP registration analyst creates an escalation request. 34. CGP operations manager triages the escalation request and makes a determination to reject or approve the CGP registration application. Go to step 32. 35. If the CGP registration application is rejected, CGP registration analyst creates a rejection report. 36. CGP registration chief QC's the rejection report.

	37. If the QC of the rejection report passes, go to step 48. If the rejection report's QC fails, the CGP registration analyst is required to make amendments, go to step 35. 38. If the CGP registration application is approved, CGP registration analyst creates an approval report. 39. CGP registration chief QC's the approval report. 40. If the approval report's QC fails, the CGP registration analyst is required to make amendments, go to step 38. 41. If the approval report's QC passes, the CGP registration chief performs some minor data entry. 42. CGP registration chief activates the organization's sites within the CGP business system. 43. CGP registration chief approves the organization and required individual SAA's. 44. CGP registration analyst finalizes the data entry. 45. CGP registration analyst creates an inspection request, which triggers the CGP inspection workflow. 46. CGP Inspection workflow is triggered (30 WF CGP Inspections). 47. CGP registration analyst creates and sends to organization registration correspondence package. 48. Process ends.
Inputs	• Organization's registration application • Individuals security assessment applications • Security checks
Outputs	• Approval or rejection of CGP registration application • CGP registration package • Triggering of various other CGP processes such as the CGP training process, CGP IAU process, etc.

1.2.2 Registration in Controlled Goods Program - Amendments

Workflow ID	**26 WF CGD Registration Amendments**
Business Unit(s)	• Registering Organization's Authorized Individual (AI) or Designated Official (DO) • CGP Program Support Clerk • CGP Program Support Information Officer • CGP Registration Coordinator • CGP Investigations and Analysis Unit (IAU) • CGP Program Management and Learning (PML) • CGP Compliance
Business Objective	• To apply amendments to an organizations CGP registered information. Can be one of the following types of amendments: o Organization termination request o Amendment to CGP information o Submission of a security assessment

	○ Submission of a business assessment ○ Submission of foreign consent ○ Submission of temporary workers or visitor exemption requests • There are five types of amendments: ○ Type 1, which are simple amendments that can be submitted through email. Includes such items as: ▪ Correction of spelling errors and/or typos ▪ Modification to the consent to post on CGP web site ▪ Remove Business Official(s) **(not AI, Owner or DO)** ▪ Removal of DO(s) **(Site requires at least one DO)** ▪ Add an approved DO to an active site ○ Type 2, which requires a security assessment application. Includes such items as: ▪ New DO's ○ Type 3, which requires an application for registration. Includes such items as: ▪ Change of address for an existing site ▪ Addition of site(s) ▪ Removal of site(s) ▪ Change of AI who will not be accessing controlled goods – remove once REG changes are approved ▪ Addition or change in Business Official(s) ▪ Change in legal name ▪ Change in business name ▪ Change in ownership (not including individuals who need to be security assessed by CGP) ▪ Amalgamation(s) of companies ○ Type 4, which requires both an application for registration and a security assessment application. Includes such items as: ▪ New Canadian Authorized Individual who will be accessing controlled goods ▪ New Canadian Owner(s) owning 20% or more of voting shares ○ Type 5, which requires other forms. Includes such items as: ▪ New foreign owner(s) owning 20% or more of voting shares (Requires the Foreign Consent form) ▪ New foreign Authorized Individual (Requiring Temporary Worker application)
Trigger	• AI or DO submission of an amendment request for any of the following reasons: ○ Organization termination request ○ Amendment to CGP information ○ Submission of a security assessment ○ Submission of a business assessment ○ Submission of foreign consent ○ Submission of temporary workers or visitor exemption requests

Workflow Description	1. Start of process 2. Applicant submits amendment request to CGP. 3. CGP program support receives and reviews the amendment submission. If the amendment is for changes to phone numbers, fax numbers or email address only, go to step 3, otherwise go to step 4. 4. CGP program support applies the amendment. Go to step 28. 5. If the amendment is a request for a temporary worker exemption, go to step 4, otherwise go to step 7. 6. The CGP IAU temporary workers exemption process is triggered (31 WF CGP Temp Worker Exemption). 7. CGP registration coordinator receives the amendment and reviews the amendment information. If the amendment information is complete go to step 9. 8. If the amendment information is deemed incomplete by the CGP registration coordinator, request information from applicant. 9. Applicant provides the requested information, go to step 1. 10. If the amendment information is complete, the CGP registration coordinator will classify the amendment. The classification of the amendment determines what inputs and actions are required for that particular amendment. 11. If the CGP registration coordinator determines it is an information only amendment, go to the next step, otherwise go to step 15. 12. The CGP registration coordinator will apply the information amendment. 13. If the information amendment does not trigger a change in risk level, go to step 15. Otherwise, the information amendment does trigger a change in risk level, the CGP registration coordinator notifies the CGP Compliance. 14. The CGP inspection process is triggered (30 WF CGP Inspections). 15. If the CGP registration coordinator determines it is an organization termination request. 16. If the amendment is for a termination, the CGP registration coordinator prepares the termination letter, which is sent to the AI or DO of the organization. 17. The CGP registration coordinator also applies the company termination amendment and terminates the organization and triggers a close-out inspection by CGP compliance, go to step 14. 18. If the CGP registration coordinator determines a security assessment is required, continue to next step, otherwise go to step 21. 19. The CGP registration coordinator conducts a security assessment. 20. CGP registration coordinator applies the security assessment information to the organization. 21. After the CGP registration coordinator performs the security assessment, if training is not required, go to step 23. 22. If the CGP registration coordinator determines that training is required, the CGP registration coordinator notifies the CGP PML. The CGP training process is triggered (28 WF CGP Designated Official Training). 23. If the CGP registration coordinator determines the amendment requires a business assessment, continue to the next step, otherwise go to step 25. 24. The CGP registration coordinator conducts a business assessment. If during the business assessment the CGP registration coordinator feels there is a need to conduct a security assessment, go to step 18.

	25. The CGP registration coordinator determines the need for an IAU for cause referral. If there is not a need for a for cause referral, go to step 27. 26. The CGP IAU for cause referral process is triggered (29 WF CGP Investigations and Analysis (IAU)). The results from the "For Cause Referral" re-triggers the need to conduct a business assessment, go to step 23. 27. CGP registration coordinator applies the business assessment amendment. 28. Process ends.
Inputs	• Submitted amendment
Outputs	• Processed amendment • Trigger of various other CGP processes.

1.2.3 Registration in Controlled Goods Program - Renewal

Workflow ID	**27 WF CGP Registration Renewal**
Business Unit(s)	• Registering Organization (Applicant) • CGP Program Support Clerk • CGP Program Support Information Officer • CGP Registration Coordinator • CGP Registration Chief • CGP Registration Analyst • CGP Operations Manager • CGP Case Management and Best Practices (CMBP) • CGP Investigations and Analysis Unit (IAU) • CGP Program Management and Learning (PML) • CGP Compliance
Business Objective	• To renew an organization's registration with the ISS Controlled Goods Program (CGP).
Trigger	• Organization requirement to renew with the ISS CGP due to being in possession or having access to controlled goods.
Workflow Description	1. Start of process. 2. CGP program support clerk creates a list of CGP registered organizations that are expiring and notifies the organization of their renewal requirements. 3. Applicant completes and submits the CGP registration application.

	4. CGP program support clerk reviews the registration application. 5. CGP program support clerk determine if all required information has been received. If all information received, go to step 7. 6. If there is missing information, CGP program support clerk requests missing information from applicant. 7. Applicant provides requested information, go to step 3. 8. CGP program support clerk performs preliminary data entry. 9. CGP program support information officer validates the application. 10. CGP program support information officer determines if all required information has been received. If all information has been received, go to step 15. 11. CGP program support information officer determines if the application is to be rejected based on the incomplete application. If the application is rejected, go to step 14. 12. If the application is not being rejected, the CGP program support information officer requests the missing information from the applicant. 13. Applicant provides the missing information. Go to step 9. 14. If the application is being rejected from step 11, CGP program support information officer notifies the applicant of the application rejection. Go to step 49. 15. If all the information was received, CGP program support clerk completes the data entry of the application. 16. CGP program support information performs a QC of the inputted data. 17. CGP program support information reviews the applicant's security assessment (SAA) as part of the application. 18. CGP program support information notifies the applicant that the CGP registration is in process. 19. CGP program support information requests security checks (Fingerprints, Criminal Record Name Check, Credit Check, etc.) as required. 20. CGP program support information notifies PML if an organization's Designated Official (DO) requires training. 21. CGP training process is triggered. (28 WF CGP Designated Official Training). 22. CGP registration coordinator triages and assigns the registration application to a CGP registration analyst for processing. 23. CGP registration analyst reviews the application and SAA for completeness. 24. CGP registration analyst determines if all required information has been received. If all the required information has been received, go to step 27. 25. CGP registration analyst requests the missing information from the applicant. 26. Applicant provides the missing information. Go to step 23. 27. CGP registration analyst completes the registration data entry. 28. CGP registration analyst analyzes the application and SAA. 29. CGP registration analyst determines if a referral to CGP investigations and analysis unit (IAU) is required. If no referral is required, go to step 31. 30. If a CGP IAU referral is required, the CGP IAU process is triggered. (29 WF CGP Investigations and Analysis (IAU)). Go to step 33.

	31. CGP registration analyst determines if a referral to CGP Case Management and Best Practices (CMBP) is required. If a CGP CMBP referral is not required, go to step 33. 32. If a CGP CMBP referral is required, the CGP CMBP process is triggered (34 WF CGP CMBP). Go to step 33. 33. CGP registration analyst receives all the results from the previous steps and determines if the CGP registration application is to be approved, rejected or if the case is high risk. If the CGP registration application is being rejected, go to step 35. If the CGP registration application is being approved, go to step 39. 34. If the CGP registration application is considered to be high risk, the CGP registration analyst creates an escalation request. 35. CGP operations manager triages the escalation request and makes a determination to reject or approve the CGP registration application. Go to step 33. 36. If the CGP registration application is rejected, CGP registration analyst creates a rejection report. 37. CGP registration chief QC's the rejection report. 38. If the QC of the rejection report passes, go to step 49. If the rejection report's QC fails, the CGP registration analyst is required to make amendments, go to step 36. 39. If the CGP registration application is approved, CGP registration analyst creates an approval report. 40. CGP registration chief QC's the approval report. 41. If the approval report's QC fails, the CGP registration analyst is required to make amendments, go to step 39. 42. If the approval report's QC passes, the CGP registration chief performs some minor data entry. 43. CGP registration chief activates the organization's sites within the CGP business system. 44. CGP registration chief approves the organization and required individual SAA's. 45. CGP registration analyst finalizes the data entry. 46. CGP registration analyst creates an inspection request, which triggers the CGP inspection workflow. 47. CGP Inspection workflow is triggered (30 WF CGP Inspections). 48. CGP registration analyst creates and sends to organization registration correspondence package. 49. Process ends.
Inputs	• Organization's registration renewal application • Individuals security assessment applications • Security checks • Other supporting documentation
Outputs	• Approval or rejection of CGP registration application • CGP registration package • Triggering of various other CGP processes such as the CGP training process, CGP IAU process, etc.

1.2.4 Registration in Controlled Goods Program- Designated Official Training

Workflow ID	28 WF CGP Designated Official Training
Business Unit(s)	• Registering Organization (Trainee) • CGP Program Support Information Officer • CGP Program Management and Learning (PML)
Business Objective	• Training of Designated Officials (DO).
Trigger	• Organization requirement to register with the CGP require at least on identified DO to have the CGP DO certification before the organization can be registered.
Workflow Description	Start of process. 1. CGP PML received notification that an individual requires the DO training. 2. CGP PML sends notification to trainee, requesting the trainee to register for the Designated Official Certification Program (DOCP) course. 3. Trainee completes course registration. 4. Trainee has 30 days to register for the course. 5. CGP PML receives all DOCP course registrations. 6. CGP PML records course registration information. 7. CGP PML reviews and validates course registration information to ensure the person registered is the same person who was invited to take the course. If course registration information is not valid, go to step 17. 8. CGP PML records the validated course registration. 9. CGP PML sends instructions to the trainee on how to retrieve the course package prior to taking training. 10. Trainee receives email to prepare for the course. If the trainee is given the opportunity to take the exam only and makes that choice, go to step 13. 11. If the trainee is not taking the exam only, the trainee will follow the instructions provided and access WebEx to download the course materials. 12. Trainee takes the DOCP training. 13. Trainee takes the DOCP exam. 14. CGP PML grades the exam. 15. CGP PML records the grades. If the trainee fails the exam on first attempt, go to step 20. If the trainee fails the exam multiple times, go to step 25. 16. CGP PML sends notification to trainee that they passed the exam and their DO certificate will be sent to them once the organization completes registration.

	17. CGP PML reviews the course registration and determines if the trainee that registered is not the same person that was invited to the training, the course registration is rejected. 18. CGP PML reject the course registration. 19. CGP PML sends notification to individual that they are not eligible to take the DOCP training. 20. CGP PML sends notification to trainee of failed exam and that they are required to exercise one of two options, retake the exam or redo the training. 21. Trainee decides to take the exam. 22. Trainee registers for exam only. 23. Trainee notifies CGP PML of decision to retake the exam. 24. Trainee decides to redo the training, go to step 2. 25. CGP PML notifies the trainee that they have failed the exam to many times and they are required to redo the training, go to step 2. 26. Trainee decides to not attend course, sends notification to CGP PML to cancel their existing course registration. 27. CGP PML cancels trainee registration. 28. CGP PML records the fact that the trainee cancelled the training. Should the trainee still require to take the training the process starts over, go to step 1. 29. Process ends.
Inputs	• New registration application with identification of DO.
Outputs	• DO certification.

1.2.5 Investigations and Analysis

Workflow ID	**29 WF CGP Investigation and Analysis (IAU)**
Business Unit(s)	• CGP Registration Analyst • CGP Inspector • CGP Case Management and Best Practices (CMBP) • CGP Investigations and Analysis Unit (IAU) Analyst • CGP Partner Organizations (e.g. RCMP, CSIS, etc.)
Business Objective	• To evaluate organization and individual security assessments, perform analysis and consult with CGP partner organizations to form a recommendation on the organization or individual in the event that the CGP registration analyst or CGP inspector are unable to satisfactorily analyze or if there is a high level of risk.
Trigger	• For cause referrals are triggered as part of the registration or inspection processes.

Workflow Description	Start of process. 1. CGP registration analyst or CGP inspector submits request for cause referral including all supporting documentation. 2. CGP IAU analyst performs an initial assessment of the for cause referral for relevance, validity and justification. If the CGP IAU analyst determines that the "For Cause Referral" is not valid, go to step 5. 3. CGP IAU analyst submits to CGP partner organizations for assessment. CGP partner organizations include RCMP, CSIS, etc. 4. CGP IAU analyst performs analysis of the "For Cause Referral" and partner organizational assessments to make a determination on impact and risk. Go to step 6. 5. CGP IAU analyst cancels the "For Cause Referral", go to step 9. 6. CGP IAU analyst determine if the referral is high risk or if there is unresolved concern, if high risk transfer file to CMBP (go to step 7), if not high risk go to step 8. 7. The CGP CMBP process is triggered (34 WF CGP CMBP). 8. CGP IAU forms a recommendation on the referral. 9. CGP IAU analyst informs initiator of the "For Cause Referral" (CGP registration analyst or CGP inspector) of the decision that the referral was not required or their recommendations. 10. CGP registration or CGP inspection receive the CGP IAU analysts cancellation notice or recommendation notice. 11. Process ends.
Inputs	• For cause referral request • Justification for referral • CGP partner assessment
Outputs	• Request for CGP partner assessment • Referral of for cause referral to CGP CMBP

1.2.6 Inspection

Workflow ID	**30 WF CGP Inspections**
Business Unit(s)	• Industry Organization • CGP Registration • CGP Management • CGP Case Management and Best Practices (CMBP) • CGP Investigations and Analysis Unit (IAU) • CGP Compliance Quality Control Officer (QC) • CGP Compliance Inspector (Inspector) • CGP Compliance Travel Coordinator • CGP Compliance Inspection Manager

Business Objective	• Complete a triggered CGP inspection.
Trigger	• An inspection can be triggered as a result of the registration process (new, renewal or amendment), termination request, CGP management requested ad-hoc inspection, incident or breach inspection request as part of an investigation or a follow-up inspection due to compliance deficiencies discovered during a previous inspection.
Workflow Description	Start of process. 1. CGP compliance QC will review and categorize received inspection request. 2. CGP compliance QC reviews list of unassigned inspection requests sorted by inspection location. 3. CGP compliance QC determines if inspection request can be deferred. If the inspection request cannot be deferred, go to step 8. 4. CGP compliance QC prepares deferral recommendation. 5. CGP compliance inspection manager reviews deferral recommendation. 6. If the CGP compliance inspection manager does not approve the deferral recommendation, go to step 8. 7. If the CGP compliance inspection manager approves the deferral recommendation, the CGP compliance QC defers the unassigned inspection request. Return to step 2. 8. CGP compliance QC reviews inspection team's individual schedules. 9. CGP compliance QC will assign request to a CGP compliance inspector based on inspection request priority, earliest diary date and similar geographical location to create an inspection request block. The diary date is the date the CGP registration is granted, for a new registration it is 90 days. 10. CGP compliance QC will repeat this process until there are no unassigned inspection requests, repeat at step 2, otherwise continue. 11. CGP compliance QC reviews the list of deferred inspections to identify those that could be used to complete an inspection request block. 12. CGP compliance QC will un-defer the inspection request and assign it to a CGP compliance inspector. 13. CGP compliance QC will repeat this process until the CGP compliance inspector's inspection request block is complete. If there is still room in the inspection request block, go to step 6, otherwise continue. 14. CGP compliance inspector reviews assigned inspection request. 15. CGP compliance inspector will submit a request to the CGP compliance QC that an inspection be reassigned to another inspector or deferred if required. 16. CGP compliance inspector will determine if the inspection request can be done via phone or requires an on-site inspection. If an on-site inspection is required go to step 17. 17. If the inspection can be completed with a phone inspection, the CGP compliance inspector will contact the organization and conduct the phone inspection. 18. If the CGP compliance inspector is successful in completing the phone inspection, go to step 52.

	19. If the CGP compliance inspector is unable to contact the inspection site by phone after several attempts, the CGP compliance inspector will send an email to the inspection site contact to confirm a date and time to which the phone inspection can be completed. Go to step 16. Otherwise, if the CGP compliance inspector was able to make contact with the inspection site, go to step 13. 20. If the CGP compliance inspector is not able to complete the phone inspection in a reasonable time frame, the CGP compliance inspector submits a request to the CGP compliance QC to pause the inspection request as they are waiting for information. This action will stop the service level clock for the inspection request. 21. If the CGP compliance inspector is still unable to make contact with the inspection site, CGP compliance inspector creates a CMBP referral and triggers the CGP CMBP process (34 WF CGP CMBP). 22. CGP compliance inspector adds inspection to their inspection schedule and enter a tentative scheduled inspection date and tentative scheduled inspection time for the request. 23. CGP compliance inspector determines if their inspection request block for on-site inspections is complete. If it is not, return to step 9 to review another inspection request. 24. Once the inspection request block for on-site inspections is deemed complete, CGP compliance inspector creates a tentative travel itinerary to be submitted to the CGP compliance travel coordinator for approval. 25. CGP compliance travel coordinator approvals the travel itinerary and makes necessary travel arrangements on behalf of the CGP compliance inspector. 26. CGP compliance inspector emails the inspection site contact to introduce themselves and arrange a date and time for the inspection. 27. CGP compliance inspector will contact the inspection site contact by phone or email to obtain answers to the questions contained within the CGP compliance pre-inspection checklist. 28. Based on the answers to the pre-inspection checklist questions, if the CGP compliance inspector determines there are no controlled goods onsite, the CGP compliance inspector will change the inspection from an on-site to phone inspection, go to step 52. 29. Based on the answers to the pre-inspection checklist questions, the CGP compliance inspector must determine if there are any amendments to the applicant's CGP registration application. If the CGP compliance inspector determines there are no application amendments, go to step 26. 30. CGP compliance inspector provides the inspection site contact with a copy of a blank registration application to be completed and sent back to the CGP. 31. If, after contacting the inspection site contact a scheduled date and time (within a reasonable time frame) cannot be arranged, the CGP compliance inspector will notify the CGP compliance QC to unassign the inspection request and will provide a date in the future when the inspection can be conducted. Go to step 2. 32. The CGP compliance inspector sends an email to the inspection site contact confirming the date and time that was arranged for the inspection. 33. CGP compliance inspector will complete sections 1 to 6 of the pre-inspection checklist for the inspection. If the pre-inspection checklist (1-6) cannot be completed, the CGP compliance inspector will re-contact the inspection site. Go to step 21.

	34. If the pre-inspection checklist (1-6) is completed, CGP compliance inspector confirms the inspection to his inspection request block. Once this task has been completed for all inspection requests assigned to the inspection block. The CGP compliance inspector sends a finalized inspection block notification to the CGP compliance inspection manager and CGP compliance QC. 35. CGP compliance inspector requests the registration files from the file room for each registrant in their inspection request block. 36. CGP compliance inspector receives the registration files. 37. The CGP compliance inspector completes sections 7 to 10 of the pre-inspection checklist for those inspections request within the inspection request block. 38. CGP compliance inspector confirms travel approval. If travel approval has not been obtained, seek travel approval. 39. CGP compliance inspector conducts the inspection. 40. CGP compliance inspector completes the inspection questionnaire. 41. CGP compliance inspector completes the compliance inspection form. 42. CGP compliance inspector completes post-inspection activities. If there were no deficiencies discovered during the site inspection, the CGP compliance inspector submits an inspection report for QC, go to step 49. 43. CGP compliance inspector notifies the inspection site of deficiencies found during the inspection and agrees with the inspection site on a reasonable date by which to have the deficiencies resolved. 44. If the deficiencies were not resolved by the agreed date, go to step 47. 45. CGP compliance inspector must determine if a follow up inspection is required. If no follow up inspection is required, the CGP compliance inspector submits the inspection report for QC, go to step 49. 46. If a follow up inspection is required, the CGP compliance inspector submits a follow up inspection request which is treated like a new inspection request, go to step 2. 47. If the identified deficiencies are not resolved in by the agreed date, the CGP compliance inspector must determine if a CMBP referral is required. If no CMPB referral is needed, the CGP compliance inspector submits the inspection report for QC, go to step 49. 48. CGP compliance inspector completes a CMBP report which then triggers the CGP CMBP process (34 WF CGP CMBP). 49. CGP compliance QC performs a QC on the inspection report, if QC passes go to step 52. 50. If the QC fails, the CGP compliance QC returns the inspection report back to the CGP compliance inspector for corrections. 51. CGP compliance inspector updates the inspection report and submits back to QC, go to step 49. 52. Process ends.
Inputs	• Inspection request from various triggers • Inspection checklist • Inspection questionnaire
Outputs	• Registrant is deemed compliant • Inspection has discovered compliance deficiencies that require action • Registrant is deemed non-compliant • CMBP referral • Inspection report

1.2.7 Temporary Workers Exemptions

Workflow ID	31 WF CGP Temporary Worker Exemption
Business Unit(s)	• Registering Organization's Designated Official (DO) • CGP Investigations and Analysis Unit (IAU) Analyst • CGP Case Management and Best Practices (CMBP) • CGP Partner Organizations (e.g. RCMP, CSIS, etc.)
Business Objective	• To process the exemption of temporary workers of an organization registered with the CGP so that the temporary workers do not need to be registered with the CGP but can still be in contact with a controlled good.
Trigger	• DO of a CGP registered organization, submitting a request for a temporary worker exemption.
Workflow Description	Start of process. 1. Organization DO submits a temporary worker request package 2. CGP IAU analyst receives the temporary worker request package and performs an initial analysis to assess relevance, validity and justification of the request. If the request is valid, go to step 4. 3. If the CGP IAU analyst determines the request was incomplete, no exemption was required or was cancelled by the DO. The CGP IAU analyst notifies the DO and original and copies of supplied supporting documentation are returned to the DO. Go to step 11. 4. CGP IAU analyst submits a referral to CGP organizational partners for an assessment. 5. CGP IAU analyst perms a detailed analysis of the temporary worker request along with the partner assessment. 6. If the CGP IAU analyst determines that the request is high risk or if there is an unresolved concern, the request is referred to CGP CMBP. 7. The CGP CMBP process is triggered (34 WF CGP CMBP). 8. CGP IAU analyst approves the temporary worker exemption without conditions, creates the exemption certificate and sends it to the DO. 9. CGP IAU analyst approves the temporary worker exemption with conditions, creates the exemption certificate along with any required conditions (such as restricted access to certain areas within the work site) and sends it to the DO. 10. CGP IAU analyst determines that the temporary worker exemption request is to be denied. The DO is notified of the denial. 11. Process ends.
Inputs	• CGP application for exemption from registration – Temporary Worker form • Temporary worker security assessment form • Copy of work permit issued by Citizenship and Immigration Canada • Original certificate of good conduct • Copy of a valid passport

Outputs	• Temporary worker exemption decision (approved, returned, denied, etc.) • Temporary worker exemption certificate (possibly with conditions based on the situation) for approved temporary workers • Letter of exemption • Letter of denial.

1.2.8 Visitor Exemptions

Workflow ID	**32 WF CGP Visitor Exemption**
Business Unit(s)	• Registering Organization's Designated Official (DO) • CGP Investigations and Analysis Unit (IAU) Analyst • CGP Case Management and Best Practices (CMBP)
Business Objective	• To process the exemption of visitors to an organization registered with the CGP so that the visitors do not need to be registered with the CGP but can still be in contact with a controlled good.
Trigger	• DO of a CGP registered organization, submitting a request for a visitor exemption.
Workflow Description	Start of process. 1. Organization DO submits a visitor request package 2. CGP IAU analyst receives the visitor request package and performs an initial analysis to assess relevance, validity and justification of the request. If the request is valid, go to step 4. 3. If the CGP IAU analyst determines the request was incomplete, no exemption was required or was cancelled by the DO. The CGP IAU analyst notifies the DO and original and copies of supplied supporting documentation are returned to the DO. Go to step 9. 4. CGP IAU analyst performs a detailed analysis of the visitor request. 5. If the CGP IAU analyst determines that the request is high risk or if there is an unresolved concern, the request is referred to CGP CMBP. The CGP CMBP process is triggered (34 WF CGP CMBP). 6. CGP IAU analyst approves the visitor exemption without conditions, creates the exemption certificate and sends it to the DO. 7. CGP IAU analyst approves the visitor exemption with conditions, creates the exemption certificate along with any required conditions (such as restricted access to certain areas within the work site) and sends it to the DO. 8. CGP IAU analyst determines that the visitor exemption request is to be denied. The DO is notified of the denial. 9. Process ends.
Inputs	• Visitor application for exemption form • Copy of valid passport • Copy of valid export permit if applicable

Outputs	• CMBP referral • Exemption certificate (with conditions were required) for approved visitors • Letter of exemption • Letter of denial

1.2.9 Industry Employee Referral

Workflow ID	**33 WF CGP Industry Employee Referral**
Business Unit(s)	• Registering Organization's Designated Official (DO) • CGP Investigations and Analysis Unit (IAU) Analyst • CGP Case Management and Best Practices (CMBP) • CGP Partner Organizations (e.g. RCMP, CSIS, etc.)
Business Objective	• DO is responsible to conduct security assessments of employees, officers and directors as well as to determine the risk of transfer posed by these employees, officers and directors. The CGP provides DO's with a Risk Management Assessment Procedure (RMAP) which is used when conducting the security assessments. Employee referrals are evaluated by the IAU and a recommendation is provided back to the DO.
Trigger	• When a DO is unable to satisfactorily conclude the security assessment for an individual or if the assessed risk level is sufficiently high.
Workflow Description	Start of process. 1. Organization DO submits an industry employee referral request package 2. CGP IAU analyst receives the employee referral request package and performs an initial analysis to assess relevance, validity and justification of the request. If the request is valid, go to step 4. 3. If the CGP IAU analyst determines the referral was incomplete, no referral was required or was cancelled by the DO. The CGP IAU analyst notifies the DO and original and copies of supplied supporting documentation are returned to the DO. Go to step 10. 4. CGP IAU analyst submits a referral to CGP organizational partners for an assessment. 5. CGP IAU analyst perms a detailed analysis of the employee referral request along with the partner assessment. 6. If the CGP IAU analyst determines that the employee referral request is high risk or if there is an unresolved concern, the request is referred to CGP CMBP. 7. The CGP CMBP process is triggered (34 WF CGP CMBP). 8. CGP IAU analyst confirms the DO's risk assessment. The CGP IAU analyst creates a referral letter and provides it to the DO. 9. CGP IAU analyst modifies the DO's risk assessment. The CGP IAU analyst creates a referral letter and provides it to the DO. 10. Process ends.

Inputs	• Employee security assessment completed by the DO • Original certificate of good conduct • Proof of citizenship • Reason for referral
Outputs	• Referral letter

1.2.10 Case Management and Best Practices

Workflow ID	**34 WF CGP CMBP**
Business Unit(s)	• Industry Organization • CGP Registration • CGP Management • CGP Case Management and Best Practices (CMBP) • CGP Investigations and Analysis Unit (IAU) • CGP Compliance Quality Control Officer (QC) • CGP Compliance Inspector (Inspector) • Policy Agencies • General Public
Business Objective	• Complete a triggered CGP Case Management and Best Practices (CMBP) Investigation.
Trigger	• A CMBP investigation can be triggered as a result of any of the other CGP processes. • CMBP investigations are triggered on an as required basis.
Workflow Description	1. Start of process. 2. CMBP referral request submitted to CMBP. 3. CMBP Manager reviews and assigns the referral to a Case Management Officer. 4. CMBP Case Management Officer creates a case file. 5. CMBP Case Management Officer determines if a violation occurred. If there was a violation continue to step 6, otherwise go to step 25. 6. CMBP Case Management Officer performs investigative procedures based on the nature of the referral. Types of referrals include, Contravention of the Defence Production Act, Omissions, Undue Risk, Compliance Issues, etc.

	7. Case Management Officer determines if the complaint submitted in the referral is founded. If the complaint is founded continue to next step, otherwise go to step 13. 8. CMBP Manager prepares a letter of intent outlining the compliant and steps to resolve. 9. CMBP Case Management Officer sends letter of intent to registrant. 10. If new information regarding the complaint is received continue to step 11, otherwise, if no new information was received go to step 14. 11. CMBP Case Management Officer performs analysis of the newly received information. 12. CMBP Case Management Officer determines if a favorable decision can be made regarding the complaint. If no favorable decision can be made, go to step 14. Otherwise continue to step 13. 13. CMBP Case Management Officer briefs the CGD on the outcome of the complaint. Go to step 25. 14. CMBP Manager prepares a recommendation to the Director of the CGP to suspend the registrant. 15. CGP Director reviews and assesses the recommendation to suspend. 16. CGP Director determines if a favorable decision can be made regarding the suspension. If no favorable decision can be made, go to step 19. Otherwise continue to the next step. 17. CMBP Case Management Officer re-instates the registrant or exemption. 18. CMBP Case Management Officer notifies the registrant of suspension. Go to step 25. 19. CMBP Manager prepares a recommendation to the Director of the CGP to revoke the registrant. 20. CGP Director reviews and assesses the recommendation to revoke. 21. CGP Director determines if a favorable decision can be made regarding the revocation. If a favorable decision regarding the revocation can be made, go to step 17. Otherwise continue to step 22. 22. CMBP Case Management Officer notifies the registrant of revocation. 23. CMBP Case Management Officer notifies the CGP Inspection of a requirement to perform a Close-Out Inspection activity. 24. The CGP Inspection process is triggered (30 WF CGP Inspections). 25. CMBP Case Management Officer closes the CMBP case file and creates CMBP report. 26. Process ends.
Inputs	• CMBP referral request
Outputs	• CMBP report. • Letter of intent to suspend/revoke. • Recommendation to suspend. • Re-instatement with CGD. • Close-out inspection.

APPENDIX 2 TO ANNEX A – KEY ACTIVITIES

APPENDIX 2 TO ANNEX A – KEY ACTIVITIES

This Appendix describes a series of key activities and associated completion dates. The schedule below is indicative of expectation and proposed approach which includes continuous communication, testing and training activities during system design and development, a pilot of the system and phased rollout of the system to its stakeholders.

Key Activities	Completion Date
Contract Award	August 2017
Planning and Analysis	December 2017
Solution Design	December 2017
Communication	March 2019 [1]
Testing	March 2019 [1]
Training	March 2019 [1]
Solution Development and Configuration	August 2018
Operational Readiness	March 2019
Implementation and Solution Pilot Launch	March 2019
Solution Pilot	June 2019
Phased Rollouts	Sept 2019
Solution Stabilization and Transition Out	December 2019
Project Closeout	December 2019

[1] Communication, Testing and Training are to start as early as possible, be recursive and targeted to audiences.

Outlined below is a very high level notion of how the project will transpire. The different phases of a typical Software Development Lifecycle are described in general terms in order to provide a sense of how the Contractor and PWGSC will interact in the development and deployment of the Solution. It should be noted that the phases below show a sequence mimicking a waterfall methodology, however, it is understood that in some cases phases and activities will be actioned in parallel.

In order for successful implementation of the Solution, a requirement for a cyclical approach for training, testing and communication will be required throughout the lifecycle of the project.

The delivery of the Solution will begin with the launch of a Pilot Phase where a part of the Solution will be made available to a select number of stakeholders, thus allowing for a final assessment of operational readiness and to work out any issues in an isolated case. Upon completion of the Pilot Phase, the Solution will move into Phased Rollouts, as the system will be introduced to remaining sets of stakeholders incrementally. The Phased Rollouts will help ensure business continuity with a gradual shift from the legacy systems supporting the ISS business to the new Solution. The Phased Rollouts will also enable the contractor to address issues in a controlled fashion than with the full Solution being in production.

The Contractor must produce, maintain, revise and deploy all deliverables that have been identified in ANNEX A in accordance with the Milestone Schedule outlined in ANNEX B. All deliverables requested must be approved by the Project Authority. Deliverables are to be delivered to the Project Authority upon completion or can be requested as per Project Authority prerogative.

1. Project Kickoff

Upon Contract Award, the project will enter the delivery stage. It is expected that there will be much collaboration required between the Contractor and PWGSC.

Immediately upon Contract Award, the Contractor must:

(a) Establish a Project Management Team;
(b) Provide the Contractor Organizational Model;
(c) Provide governance model; and
(d) Hold a Project Kick-off session.

2. Planning Phase

During this phase, the Contractor and PWGSC will review the requirements and business processes to ensure there is a complete and accurate understanding. Business Process Re-Engineering, Communications, training, testing, change and project management planning will commence. These plans must include timeframes, target audiences, potential risks and their mitigation strategies as well as a description of the activities as indicated within the requirements found within ANNEX A. The timeframes must align with the Key Activities outlined above.

At the end of this phase, the Contractor must:

(a) Refine Communications and Change Management Strategies and Plans;
(b) Develop and provide a Risk Register itemizing risks, mitigation strategies and actions taken for the project;
(c) Provide an Issue Log itemizing issues and associated action items for the project;
(d) Refine the Project Management Plan;
(e) Develop and provide a high-level Project Schedule for the delivery of the requirements;
(f) Provide Business Process Re-Engineering Strategy and Plan;
(g) Provide Solution Delivery Plan; and
(h) Provide a Data Migration Strategy and Plan.

3. Analysis Phase

During this Phase, there will be an opportunity for the Contractor, with their expertise and knowledge of the case management tool, as well as their newly gained appreciation of the requirements, to challenge and recommend changes to the business processes to improve effectiveness and efficiency.

At the end of this Phase, the Contractor must:

(a) Launch of Communications, Testing, Training and Change Management Cycles;
(b) Analyze and redesign current As Is business processes;
(c) Propose changes to and update the business process maps once approved by PWGSC;
(d) Develop the business architecture for the Solution;
(e) Contribute towards the completion of Gate 1 of SA&A process as outlined in Section 5, 1.1.1 of ANNEX A;
(f) Develop Operational Readiness Plan;
(g) Refine the Data Migration Plan;
(h) Refine the Business Process Re-Engineering Plan;
(i) Refine the Solution Delivery Plan;

4. Design Phase

Following the completion of the Analysis Phase, the Solution Design must be refined and detailed. The Contractor must develop a Logical Solution Architecture of the IT solution in collaboration with Enterprise Architecture at PWGSC. The Architecture must provide more details of the Solution to be implemented and must cover the business, application, data, and technology and security architecture views. PWGSC will facilitate and coordinate all communication and activities with Shared Services Canada who will support and own the infrastructure components such as data centres, servers, networking and infrastructure security.

The Contractor must:

(a) Deliver the Solution Architecture at a logical level for approval by the PWGSC Architecture Review Board;
(b) Deliver Access Control and User Management Plan;
(c) Update the Project Management Plan;
(d) Refine Communications, Training and Testing Plans;
(e) Refine Change Management Plan;

5. Development Phase

Once the design has been completed and approved, the technology must be developed, configured and integrated as per the Solution Architecture specifications and the approved business processes. The objective is to configure the Solution as per the requirements set out in ANNEX A and those that have been refined and approved during the planning and design phases.

The Contractor must:

(a) Refine test plan and test cases in alignment with the Solution requirements for system testing, user acceptance testing, performance testing and load testing;
(b) Develop and provide Security Assessment Plans for approval;
(c) Refine Operational Readiness Plan;
(d) Provide Detailed Design Specifications;
(e) Refine Solution Delivery Plan;
(f) Refine Access Control and User Management Plan;
(g) Develop plan for implementation of the Solution Pilot;

6. Testing Phase

In accordance with the testing requirements set out in ANNEX A, all testing must be completed before the Solution is deployed to production. The Contractor must refine the Solution Test Plan and test cases in accordance with the Solution requirements.

The Contractor must:

(a) Execute the testing plan and provide system, unit, functional, end to end, security, performance and load test results for approval;
(b) Provide the completed requirements traceability matrix;
(c) Complete Gate 2 of the SA&A process;

7. Training Phase

In accordance with the training requirements set out in ANNEX A, all training must be completed before the Solution is deployed to production.

The Contractor must:

(a) Execute the training plan;
(b) Refine Operational Readiness Plan;
(c) Execute Operational Readiness Assessment;

8. Operational Readiness/Solution Implementation

The Solution go-live date for the Pilot Phase is March 31, 2019 to an identified set of users. Upon completion of the pilot phase, the Contractor must ensure operational readiness prior to commencing with the Solution's phased rollout. The Phased rollout will introduce the Solution to the remaining users through incremental deployment between the months of June and September 2019.

The Contractor must:

(a) Completion of all testing activities.
(b) Report demonstrate testing success by providing test case evidence for system testing (end to end), user acceptance testing and performance testing;
(c) Completion of all training of business and technical resources as planned;
(d) Document feedback from trainees on success of training;
(e) Assess and report on the success of training;
(f) Delivery of training artifacts such as GC-accessible knowledge base, process oriented end to end Standard Operating Procedures, content for training modules for redistribution, reference materials, functional specifications;
(g) Identify and document outstanding system defects;
(h) Identify and document solution shortfalls;
(i) Completion of all communication activities;
(j) Provide an in service support plan which includes knowledge transfer for operations;
(k) Complete Gate 3 of the SA&A process;
(l) Launch Pilot Phase;
(m) Launch Phased Solution Roll-out post successful Pilot;
(n) Update the Risk Register and Issue Log; and
(o) Update the detailed Project Schedule.

9. Stabilization and Transition-Out

During this period of nine (9) months following solution launch, the Contractor must continue to support the Solution in all areas described in ANNEX A, such as training, communications, change management and correcting defects. As well, the Contractor must ensure a smooth transition of the support activities to PWGSC during this phase.

The Contractor must:

(a) Deliver a Project Close-Out Document;
(b) Deliver a Lessons-Learned Document;
(c) Execute knowledge transfer;
(d) Deliver Build Books related to the Solution;

(e) Deliver all training, communications, business processes, change management and testing documentation; and
(f) Deliver documented future recommendations.

APPENDIX 3 TO ANNEX A – USER ACCOUNTS OVERVIEW

APPENDIX 3 TO ANNEX A - USER ACCOUNTS OVERVIEW

This appendix provides a high level description of main user account types for the solution described in ANNEX A.

1. EXTERNAL USERS

The Industrial Security Sector (ISS) Clients and Partners which are described herein as External Users will be able to access ISS services through the Solution's Web Portal.

1.1 Company Security Officer (CSO)

A CSO is a Canadian citizen or permanent resident, employed by a private sector organization that is registered into the Contract Security Program (CSP). The CSO is responsible for monitoring the organization's security profile, addressing security issues, and is accountable to the CSP and to the organization's designated Key Senior Official on all industrial security matters. The CSO is the organization's point of contact with the CSP. The user account for CSOs are created by the ISS. CSOs can request the creation of user accounts for Applicants and other CSOs.

Service	Actions Permitted
General	1) Update identification credentials; 2) Update account profile/preferences; 3) View guidelines and forms; 4) Receive general notification from CSP; 5) Send notification to CSP; 6) Electronic signature/electronic consent; 7) Generate reports; 8) View/set Calendar events;
Registration in the CSP	1) Submit service requests for completion or renewal of organization's registration with CSP (e.g., Designated Organization Screening (DOS), Facility Security Clearance (FSC), Document Safeguarding Capability (DSC), Production Capability, Shredding Capability, Bulk Storage Capability, and IT Security); 2) Submit supporting documentation (as required by CSP); 3) Receive case specific notification from CSP; 4) Send case specific notification to CSP; 5) View case specific documents issued by CSP; 6) Track status of Registration/Renewal service requests; 7) Search/View past Renewal service requests completed.
Personnel Security Screening	1) Request creation of Applicant accounts; 2) Request creation of CSO accounts; 3) Submit Requests for Personnel Security Screening services (New, Update, Upgrade, Transfer, Duplication, Re-activation, Termination); 4) Complete PSS requests for herself/himself and on behalf of Applicants; 5) Track completion status of Personnel Security Screening service requests; 6) Send/receive case specific notifications to/from CSP; 7) Forward to Applicants case specific notification received from CSP; 8) View/Delete/Submit Applicants' supporting documents to CSP; 9) View CSP documents (Briefing Certificates, etc.); 10) Search past PSS requests completed.
Subcontracting	1) Complete/Update/Submit SRCLs; 2) Complete/Update/Submit Private Sector Organization Screening;

	3) Submit supporting documentation (as required by CSP); 4) View case specific documents issued by CSP (e.g., Security Clauses, Subcontractor's organization security clearance and individual clearances, etc.); 5) Receive case specific notification from CSP; 6) Send case specific notification to CSP; 7) Track status of service requests; 8) View past service requests (completed).
Request for Visit	1) Submit Request for Visit service requests; 2) Submit Amendments (Renewals/Additions/Deletions) to Requests for Visit service requests; 3) Submit supporting documentation (as required by CSP); 4) View CSP documents (e.g., Authorized Visit request clearance Form, Letter of rejection, etc.); 5) Receive case specific notification from CSP; 6) Send case specific notification to CSP; 7) Track completion status of RFV service requests; 8) Search/View past RFV (completed).
Documents Transfer	1) Send notification of documents transfer; 2) Submit supporting documentation (as required by CSP); 3) Receive case specific notification from CSP; 4) View case specific documents issued by CSP; 5) Track status of Documents Transfer service request; 6) View/Search past Documents Transfer information.
Report Security Breaches	1) Send notification of security breach to CSP; 2) Submit supporting documentation (as required by CSP); 3) Receive case specific notification from CSP; 4) View case specific documents issued by CSP;

1.2 GC-Security Officer (GC-SO)

The GC-SO is a Security Officer of a Government organization that collaborates with ISS. The GC-SO is the organization's point of contact with the CSP. The GC-SO user accounts are created by the ISS. The GC-SOs can request the creation of user accounts for Applicants and for other GC-SOs. Before requesting the creation of Applicant/CSO accounts, the requestor is responsible for verifying their identity and to provide CSP the tombstone user identification information necessary for the account creation.

Service	Actions Permitted
General	1) Update account profile/preferences; 2) Update identification credentials; 3) View guidelines and forms; 4) Receive general notification from CSP; 5) Send notification to CSP; 6) Electronic signature/electronic consent; 7) Generate reports; 8) View/set Calendar events.
Sponsor an Organization	1) Submit Private Sector Organization Screening (PSOS) service requests; 2) Submit supporting documentation (as required by CSP); 3) Track status of Registration service requests; 4) Receive case specific notification from CSP;

	5) Send case specific notification to CSP; 6) View case specific documents issued by CSP; 7) Search past Sponsoring service requests (completed).
Personnel Security Screening	1) Request creation/deletion of Applicant accounts; 2) Send case specific notification to Applicant; 3) Receive case specific notification from Applicant; 4) View/ Delete/Submit Applicants' PSS request and supporting documents to GC-SO organization`s IT system;
Request for Visit	1) Submit Request for Visits service requests; 2) Submit Amendments (Renewals/Additions/Deletions) to Requests for Visit service requests; 3) Submit supporting documentation (as required by CSP); 4) View CSP documents (e.g., Authorized Visit request clearance Form, Letter of rejection, etc.); 5) Receive case specific notification from CSP; 6) Send case specific notification to CSP; 7) Track completion status of RFV service requests; 8) Search/View past RFV (completed).

1.3 Applicant

The Applicant is an employee of a private sector organization registered with CSP, or an employee of a GC organization. The Applicant user account is initiated by CSO or GC-SO and completed by ISS.

Service	Actions Permitted
General	1) Update identification credentials; 2) Update account preferences; 3) View guidelines and forms; 4) Receive general notification from CSP; 5) Electronic signature/electronic consent
Personnel Security Screening	1) Complete Personnel Security Screening Requests online; 2) Submit supporting documentation (if required); 3) Receive case specific notification from CSO or GC-SO; 4) View case specific documents issued by CSO or GC-SO; 5) Send case specific notification to CSO or GC-SO; 6) Track status of service requests; 7) View past PSS Request completed.

1.4 Foreign Security Officer (FSO)

The Foreign Security Officer is a National Security Authority or Designated Security Authority of another country. The FSO user accounts are created by the ISS.

Service	Actions Permitted
General	1) View guidelines and forms; 2) Update account profile/preferences; 3) Update identification credentials; 4) Receive general notification from CSP; 5) Send notification to CSP;

	6) Electronic signature/electronic consent; 7) Generate reports 8) View/set Calendar events
Request for Visit	1) Submit Request for Visit service requests 2) Submit Amendments (Renewals/Additions/Deletions) to Requests for Visit service requests 3) Submit supporting documentation (as required by CSP) 4) View CSP documents (e.g., Authorized Visit request clearance Form, Letter of rejection, etc.) 5) Receive case specific notification from CSP 6) Send case specific notification to CSP 7) Track completion status of RFV service requests; 8) Search/View past RFV (completed)
Sponsor an Organization	1) Submit Private Sector Organization Screening (PSOS) service requests; 2) Submit supporting documentation (as required by CSP) 3) Track status of Registration service requests 4) Receive case specific notification from CSP 5) Send case specific notification to CSP 6) View case specific documents issued by CSP 7) Search past Sponsoring service requests completed

1.5 Procurement Officer (GC-PO)

The GC-PO is a GC procurement officer who carries out specialized advanced purchase of goods and services, or a GC project manager leading a project on which Industry organizations have a bid or intend to bid. The GC-PO user accounts are created by the ISS.

Service	Actions Permitted
General	1) Update account profile/preferences 2) Update identification credentials 3) View guidelines and forms 4) Receive general notification from CSP 5) Send notification to CSP 6) Electronic signature/electronic consent; 7) Generate reports 8) View/set Calendar events
Sponsor an Organization	1) Submit Private Sector Organization Screening (PSOS) service requests; 2) Submit supporting documentation (as required by CSP) 3) Track status of Registration service requests 4) Receive case specific notification from CSP 5) Send case specific notification to CSP 6) View case specific documents issued by CSP 7) Search past Sponsoring service requests (completed)
Contract Security	1) Complete and submit SRCLs; 2) View/Update SRCLs; 3) Submit contract information; 4) Update contract information (amendments); 5) Submit supporting documentation (if required); 6) View case specific documents issued by CSP (e.g., Security Clauses); 7) Receive case specific notification from CSP;

	8) Send case specific notification to CSP; 9) Track status of service requests; 10) View past service requests (completed).

1.6 Authorized Individual (AI)

An Authorized Individual is a Canadian citizen or permanent resident ordinarily residing in Canada that operates a business in Canada or is the representative of a business that seeks/maintains registration with the Controlled Goods Program. The AI user account is created by the ISS. AIs can initiate the creation of Designated Official (DO) user accounts.

Service	Actions Permitted
General	1) Update identification credentials; 2) Update account profile/preferences; 3) View guidelines and forms; 4) Receive general notification from CGP; 5) Send notification to CGP; 6) Electronic signature/electronic consent; 7) Generate reports; 8) View/set Calendar events.
Registration	1) Complete/Maintain Registration in CGP; 2) Submit supporting documentation (e.g., Security Assessment Application, etc.); 3) Receive case specific notification from CGP; 4) Send case specific notification to CGP; 5) View case specific documents issued by CGP (e.g., copy of Certificate of Registration, etc.); 6) Track status of Registration/Renewal service requests; 7) Search/View past Renewal service requests completed;
Appointment of DO	1) Request creation of Designated Official accounts; 2) Submit Request for CGP vetting the appointment of a DO; 3) Submit supporting documentation (if required); 4) Receive case specific notification from CGP; 5) Send case specific notification to CGP; 6) View case specific documents issued by CGP (e.g., Letter of Acceptance, copy of Designated Official Certification Program certificate, etc.); 7) Track status of registration/DO vetting service request; 8) Search/View past service requests.
Report Security Breaches	1) Submit Security Breach Report; 2) Submit supporting documentation (as required by CGP); 3) Receive case specific notification from CGP; 4) Send case specific notification to CGP; 5) View case specific documents issued by CGP;

1.7 Designated Official (DO)

A Designated Official (DO) is a Canadian citizen or permanent resident ordinarily residing in Canada who : 1) is an employee of an organization registered with CGP; 2) has been appointed by a CGP Authorized Individual; 3) has been authorized by the CGP and 4) has completed the CGP's Designated Official Certification Program. The DO is

the organization's point of contact with the CGP. The creation of DO user account is initiated by AI and completed by ISS.

Service	Actions Permitted
General	1) Update identification credentials; 2) Update account profile/preferences; 3) View guidelines and forms; 4) Receive general notification from CGP; 5) Send notification to CGP; 6) Electronic signature/electronic consent; 7) Generate reports; 8) View/set Calendar events.
Exemptions from Registration in the CGP	1) Submit Applications Exemption from Registration (Visitor/Temporary Worker); 2) Submit supporting documentation (e.g., Security Assessment Application, etc.) 3) Receive case specific notification from CGP; 4) Send case specific notification to CGP; 5) View case specific documents issued by CGP; 6) Track status of Registration/Renewal service requests; 7) Search/View past Renewal service requests completed;
Referrals to the CGP	1) Requests CGP assistance in completing employee determination; 2) Submit supporting documentation (e.g., Security Assessment Application, proof of citizenship, CRNC, etc.); 3) Receive case specific notification from CGP; 4) Send case specific notification to CGP; 5) View case specific documents issued by CGP; 6) Track status of Referral service requests; 7) Search/View past Referral service requests completed.
Report Security Breaches	1) Submit Security Breach Report; 2) Submit supporting documentation (as required by CGP); 3) Receive case specific notification from CGP; 4) Send case specific notification to CGP; 5) View case specific documents issued by CGP; 6) Track status of Registration/Renewal service requests

2. INTERNAL USERS

An Internal User is an employee of the Industrial Security Sector that is responsible for processing services requests in support of CSP or CGP. The scope of Internal User accounts is limited to accessing the Services Processing Application. The user account for ISS Internal Users are created by the ISS Information System Security Officer. The access level and privileges of ISS Internal Users are to be aligned with their operational requirements and authorization.

The following are examples of generic Roles and Responsibilities, Access Levels and Privileges that apply to ISS Internal Users.

2.1 Generic Roles

Contracts Security Program	
Functional Area	**Generic Role**
Contracts Security	Manager, Contract Security
	Chief, Contract Security
	Contract Security Officer
	Visit and Document Control Officer
	Documentation Control Officer
	Quality Control Officer
Registration	Manager, Registration
	Chief, Registration
	Registration Analyst
Inspections and Investigations	Manager, Inspections and Investigations
	Chief, Inspections/Investigation
	Chief, Resolution of Doubt
	IT Security Inspector
	Field Industrial Security Officer
	Resolution of Doubt Officer
Personnel Security Screening	Manager, Personnel Security Screening
	Chief, Personnel Security Screening
	Head, Personnel Security Screening
	Personnel Security Screening Specialist

APPENDIX 4 TO ANNEX A – LEGISLATIVE, REGULATORY AND POLICY REQUIREMENTS

APPENDIX 4 TO ANNEX A – LEGISLATIVE, REGULATORY AND POLICY REQUIREMENTS

This Appendix outlines the Legislative, Regulatory and Policy requirements and related references applicable to the Work described in *ANNEX A – Statement of Work (SOW)*. The Contractor and the Solution must comply directly with all relevant federal legislation, regulations, policies, directives, standards and guidelines including (but not limited to) those described into this APPENDIX.

1. INTRODUCTION

Legislation, regulations, policy, directives, standards and guidelines provide further useful information to determine the compliance requirements of the Solution and of the delivery of services to GC, as well as the scope and complexity of the business workflow and functional requirements that must be implemented.

While the current location of the latest electronic version of each document is provided, all are subject to change and the Solution must facilitate GC's continued compliance with all legislative, regulatory and policy requirements.

2. ACTS AND REGULATIONS

The services delivered through the Solution must facilitate compliance with all GC policies, directives and guidelines, including but not limited to:

Financial Administration Act	http://laws-lois.justice.gc.ca/eng/acts/f-11/
Access to Information Act	http://laws-lois.justice.gc.ca/eng/acts/a-1/
Privacy Act	http://laws-lois.justice.gc.ca/eng/acts/p-21/
Personal Information Protection and Electronic Documents Act (PIPEDA)	http://laws-lois.justice.gc.ca/eng/acts/p-8.6/
Library and Archives of Canada Act	http://laws-lois.justice.gc.ca/eng/acts/l-7.7/
Official Languages Act	http://laws-lois.justice.gc.ca/eng/acts/o-3.01/
Defence Production Act	http://laws-lois.justice.gc.ca/eng/acts/d-1/
Visiting Forces Act	http://lois-laws.justice.gc.ca/eng/acts/V-2/
Criminal Code	http://laws-lois.justice.gc.ca/eng/acts/c-46/
Canada Evidence Act	http://laws-lois.justice.gc.ca/eng/acts/C-5/
Criminal Records Act	http://laws-lois.justice.gc.ca/eng/acts/c-47/
Export and Import Permits Act	http://laws-lois.justice.gc.ca/eng/acts/e-19/
Controlled Goods Regulation	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/
Secure Electronic Signature Regulations	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html

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

3. POLICIES, DIRECTIVES, STANDARDS AND GUIDELINES

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

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
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
Policy on Government Security	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578
Directive on Departmental Security Management	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579
Operational Security Standard: Management of Information Technology Security (MITS)	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328
Operational Security Standard on Physical Security	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329
Standard on Security Screening	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115
Security and Contracting Management Standard	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12332
Operational Standard for the Security of Information Act	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12323
Security Organization and Administration Standard	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12333
Policy on Financial Management Governance	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14005
Policy on Internal Audit	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484
Policy on Communications and Federal Identity	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30683
Federal Identity Program Policy	ww.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/fip-pcim/index-eng.asp
Directive on Identity Management	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577
Directive on the Administration of the Access to Information Act	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310
Directive on Management of Information Technology	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249
Policy on Acceptable Network and Device Use	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122

All other Treasury Board policies and related instruments including those not listed above, can be found in their entirety on the Treasury Board of Canada Secretariat website (http://www.tbs-sct.gc.ca/pol/index-eng.aspx).

4. POLICIES, STANDARDS AND DIRECTIVES GOVERNING ON-LINE SERVICE DELIVERY

The Contractor and Solution must comply directly with all relevant federal policies, directives and guidelines related to on-line service delivery, including but not limited to:

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 Web Interoperability	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25875
Standard on Optimizing Websites and Applications for Mobile Devices	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27088
Technical specifications for the Web and mobile presence	http://www.tbs-sct.gc.ca/ws-nw/mo-om/ts-st/index-eng.asp
Standard on Privacy and Web Analytics	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26761

Standard on Email Management	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27600

All other Treasury Board web communication instruments including those not listed above, can be found in their entirety on the Treasury Board of Canada Secretariat website (http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/index-eng.asp).

5. IT SECURITY GUIDELINES

The Contractor and Solution must follow the Government and industry general accepted IT security guidelines, including but not limited to:

ITSG-33 IT Security Risk Management: A Lifecycle Approach	https://www.cse-cst.gc.ca/en/node/265/html/22814
ITSG-41 Security Requirements for Wireless Local Area Networks	https://www.cse-cst.gc.ca/en/node/264/html/15287
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-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-31 User Authentication Guidance for IT Systems	https://www.cse-cst.gc.ca/en/node/267/html/22784
ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada	https://www.cse-cst.gc.ca/en/node/268/html/15236
ITSP.30.031 V2 User Authentication Guidance for Information Technology Systems	https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng.pdf
Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information	https://www.cse-cst.gc.ca/en/node/1831/html/26515
User Authentication Guidance for Information Technology Systems	https://www.cse-cst.gc.ca/en/node/1842/html/26717
Clearing and Declassifying Electronic Data Storage Devices	https://www.cse-cst.gc.ca/en/publication/itsg-06
NIST SPECIAL PUBLICATIONS (SP)	http://csrc.nist.gov/publications/PubsSPs.html#SP 800

All CSE guidelines, including those not listed above, can be found in their entirety on the *IT Security Guidance* Section of CSE website (https://www.cse-cst.gc.ca/en/group-groupe/its-advice-and-guidance).

6. CONTRACT SECURITY PROGRAM - FORMS AND GUIDELINES

The Contractor and Solution must comply directly with all relevant Contract Security Program – Forms and Guidelines, including but not limited to:

Industrial Security Manual	
Industrial Security Manual	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/index-eng.html
Personnel Security Screening	
Personnel Screening, Consent and	http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-eng.asp

Authorization form (TBS/SCT 330-23E)	
Security Clearance form (TBS/SCT 330-60E)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-60-eng.asp
Security Screening Certificate and Briefing form (TBS/SCT 330-47)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-47-eng.asp
Security Requirements Check List (TBS/SCT 350-103)	http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-eng.asp
Company security officer and alternate company security officer security incident report	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/rapport-incident-report-eng.html
Company security officer or alternate company security officer attestation form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/attestation-eng.html
Consent to release of reliability screening and/or security clearance information	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/cnsntmnt-cnsnt-eng.html
Personnel security screening forms tips	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/conseils-tips-eng.html
Personnel security clearance form checklists	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/liste-checklist-eng.html
Personnel security clearance form most common mistakes	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/erreurs-mistakes-eng.html
Contract Security	
Security Requirements Check List (TBS/SCT 350-103)	http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-eng.asp
Organization Security Screening	
Request for Private Sector Organization Screening form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/esosp-psos-eng.html
Annex 1-A – Corporate company security officer / company security officer security appointment and acknowledgement and undertaking	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-1a-eng.html
Annex 1-B – Alternate company security officer security appointment and acknowledgement and undertaking	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-1b-eng.html
Annex 3-G – Public Works and Government Services Canada – Security agreement	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3g-eng.html
Annex 3-D – Resolution for the exemption of parent organization	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3d-eng.html
Annex 3-E – Non-Disclosure certificate	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3e-eng.html
Annex 3-F – Subsidiary board resolution noting parent's exclusion and resolution to exclude parent organization	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3f-eng.html
How to complete a Request for Private Sector Organization Screening form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/esosp-psos-instructions-eng.html
Organization Safeguarding	
Annex 5-A – Registering document for equipment purchase	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5a-eng.html
Transport and transmittal	

Appendix A-1 to annex 5-D – Courier certificate/itinerary	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a1-eng.html
Appendix A-3 to annex 5-D – Pre-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a3-eng.html
Appendix A-3 to annex 5-D – Pre-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a3-eng.html
Appendix A-4 to annex 5-D – Post-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a4-eng.html
Guideline for suggested transportation plan content	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/pt-tp-eng.html
Guideline for suggested notice of classified consignment	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/avis-notice-eng.html
Visits	
Request for visit (Domestic and International)	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/visite-visits-eng.html
Instructions for completing the domestic request for visit form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/domestique-domestic-eng.html
Instructions for completing the international request for visit form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/internationale-international-eng.html

All other Contract Security Program forms and guidelines including those not listed above, can be found on the Industrial Security website (http://iss-ssi.pwgsc-tpsgc.gc.ca/psi-isp-eng.html).

7. CONTROLLED GOODS PROGRAM - FORMS AND GUIDELINES

The Contractor and Solution must comply directly with all relevant Controlled Goods Program – forms and Guidelines, including but not limited to:

Registration	
Application for registration	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/inscription-registration-eng.html
Security assessment application - owner, authorized individual, designated official, officer, director, employee	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/des-saa-eng.html
Security assessment summary by designated official conducting a security assessment of an employee, director or officer	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/ses-sas-eng.html
Guideline on Controlled Goods Program registration	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/inscription-registration-eng.html
Guide to the New Schedule to the Defence Production Act	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/lpd-dpa-toc-eng.html
Inspections and Compliance	
Guideline on Controlled Goods Program compliance inspections	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/inspections-eng.html
Pre-inspection self-assessment checklist	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ressources-resources/publications/pre-inspection-eng.html
Security breach report form	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/as-sbr-eng.html
Registration Exemptions	

Application for exemption for registration—temporary worker/international student	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/travailleur-worker-eng.html
Visitor application for security assessment and exemption from registration form	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/visiteurs-visitors-eng.html
Security assessment application—temporary worker/international student	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/des-travailleur-saa-worker-eng.html
Designated Officials	
Designated Official Certification Program	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/formation-training-eng.html
Guideline for Designated Officials	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/rd-directives-do-guidelines-eng.html

All other Controlled Goods Program forms and guidelines including those not listed above, can be found on the Controlled Goods Program website (http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/index-eng.html).

APPENDIX 5 TO ANNEX A – GLOSSARY OF TERMS

APPENDIX 5 TO ANNEX A – GLOSSARY OF TERMS

This Appendix outlines key terms that are employed throughout *ANNEX A – Statement of Work (SOW)*. This Appendix should be used in conjunction with *APPENDIX 6 to ANNEX A: Acronyms and Abbreviations*.

A

Acceptance Test Plan: 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 Solution.

Access Right(s): An approach to control, regulate or restrict system access to a User according to the User's assigned role(s) and privileges.

Authorized Administrator: IA user role defined and authorized to manage advanced system functionalities in the Solution, such as configuration of business rules, workflows, etc.

Authorized Individual: Canadian citizen or permanent resident ordinarily residing in Canada that carry on a business in Canada or is the representative of a business that seeks/maintain registration with Controlled Goods Program.

Authorized User: A user role authorized to perform operations in the Solution.

Analytics: The application of mathematical formulas, statistics, queries, info cubes and other data objects to analyze various aspects of the Solution.

Applicant: An employee of a private sector organization registered with CSP, or an employee of a Government organization that collaborates with CSP for Personnel Security Screening Services.

Application Programming Interface (API): 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 security credentials (e.g., digital identity) of a User of the Solution.

B

Boolean Catalogue Search: A type of search that can combine words and phrases using AND, OR, NOT (known as Boolean operators) to limit, broaden, or define the search.

Business Day: 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.

C

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.

Classified Information: Information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest. Classification categories include 'Confidential', 'Secret', or 'Top Secret' (see designated information).

Classification Level: An indicator of the sensitivity of information in the Solution (e.g. Protected A, Protected B, Unclassified, and other classifications specified by Government of Canada (GC)).

Client: An External User within the context of the Solution.

Confidentiality: The sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of injury should unauthorized disclosure occur.

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.

Control Test Environment: The equivalent of a User Acceptance Test (UAT) or Pre-Prod environment.

Controlled Goods: The goods as defined under the schedule to the Defence Production Act and listed in the schedule to the Export Control List under section 3 of the Export and Import Permits Act.

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.

Cryptography: The discipline that treats the principles, means, and methods for safeguarding plain information by making it unintelligible. It also means reconverting the unintelligible information into intelligible form (see encryption).

Customer: The ultimate recipient of the system integrator professional services.

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.

D

Data Architecture: The architecture 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.

Delivery Stage: see National Project Management Strategy (NPMS). The purpose of the Project Delivery Stage is to translate the approved project objectives and requirements into technical criteria to allow for detailed design and full implementation of the end product. The project team will build, test, implement and transfer the project's product, service or result to operations, and will close out the project smoothly, transferring any outstanding issues to operational OPIs.

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).

Design Specification: The activities and deliverables associated with translating User and information system requirements into detailed technical specifications.

Designated information: Information related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act. Categories include: ‘Protected A’ for sensitive, ‘Protected B’ for particularly sensitive, or ‘Protected C’ for extremely sensitive (see classified information).

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.

Document Management: 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.

Duplication of Security Screening/Clearance: The security clearance or reliability status of an individual contractor employed by multiple registered organizations may be duplicated provided the following criteria are met: 1) the screening is still valid; the screening is not due for updating; the organization requesting the duplication is registered and in good standing in the Contract Security Program

E

Electronic Data Interchange (EDI): 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.

Encryption: The transformation of readable data into an unreadable stream of characters using a reversible coding process (see cryptography).

Enterprise Service Bus (ESB): A software architecture model used for designing and implementing communication between software applications in a service-oriented architecture (SOA).

External User: See User. Non-ISS users who access the ISS services facilitated by the Solution. Example of External Users roles include Company Security Officers, GC Security Officers, GC Procurement Officers, Foreign Security Officers, Designated Officials, etc.

F

File Archiving: The removal of a record from the production data such that it can no longer be accessed or modified.

Foreign Security Officer (FSO): A foreign officer designated as the National Security Authority or Designated Security Authority of another country.

Fuzzy Logic Search: A text retrieval technique based on finding matches even when keywords are misspelled or only hint of a concept.

G

GC-Security Officer (GC-SO): The GC-SO is a Security Officer of a Government organization that collaborates with ISS. The GC-SO is the organization's point of contact with the CSP. For the purpose of the Solution, the GC-SO is an External User.

Generic accounts: any accounts 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.

H

Host: Means any Internet Protocol (IP) addressable entity connected to an IP-based network.

I

Incident: 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: The Incident Management process is responsible for managing the lifecycle of all IT incidents impacting production application and services. This ensures that normal service operation is restored as quickly as possible and minimizes the adverse impact on business operations thereby ensuring that expected levels of service quality are maintained.

Information Protection Centre (IPC): A GC's point of contact for security incidents.

Information System Security Officer (ISSO): A privileged User role defined and authorized for managing the Access Control in the Solution. ISSO creates, modifies, disables, deletes and audits users' accounts for Internal and External Users.

Integration: The process of bringing together the component subsystems into one system and ensuring that the subsystems function together as a system.

Integrity: The accuracy and completeness of information and assets and the authenticity of transactions.

Internal User: See User. ISS employees who utilize the Solution to deliver the CSP/CGP services to External Users. Example of Internal Users include Registration Officers, Personnel Security Screening Officers, Inspectors, Investigators, etc.

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 the Solution, 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.

Intuitive interface: Solution interfaces that are intuitive, as defined above ("Intuitive"), for both the Web Portal and Services Processing Application portions of the Solution.

ISS Data: All data associated with the Solution.

ISS Infrastructure: All hardware, systems software, and facilities that process and manage the Solution.

ISS Management Data: Any data derived from the operation, administration and management of the Solution that the Contractor directly uses for:

a) service requests;
b) incident tickets (excluding security incident tickets);
c) asset records;
d) configuration records;
e) system performance, capacity and resource planning information; and
f) alarms and events (excluding security alarms and events).

ISS System Data: Any data that the Contractor uses to control or modify the operation, administration and management of the ISS 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.

ISS User Data: Any data that includes Account, Notifications, Customized views and filters.

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: The process which institutionalizes best practices, training materials, and organizational policies for quick and easy access.

L-M

Least privilege: Security principle according to which the Solution users must be provided with the least amount and types of system privileges that still provides them with an unimpeded ability to perform their jobs.

Malware: Any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It 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.

Metrics: Measures of performance that observe progress and evaluate trends within an organization.

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.

N

National Project Management Strategy: The National Project Management System is PWGSC's project management framework for *Real Property Projects* and *IT-Enabled Projects*. The NPMS framework defines key principles and provides the directives, roadmaps, deliverables and tools needed to successfully deliver projects on scope, on time and on budget.

Near Real-Time (NRT): The time delay introduced by automated data processing or network transmission, between the occurrence of an event and the use of the processed data, such as for display or feedback and control purposes.

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”.

Notification: Message informing a User of an action required (e.g. approve, deny, send supporting documentation, etc.) or that an action has been completed that requires attention. Notifications could be system generated by the Solution or messages that are customized by the Internal Users

O

Online Industrial Security System (OLISS): An online web application for submission of personnel security clearance requests.

Open Data: A practice that makes data easily available to the public in order to enable re-use of the data.

Other Government Departments (OGD): Any Department and Agency other than Public Works and Government Services Canada.

P

Patch Management: Standardized methods and procedures to minimize the impact of problems for the Solution.

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.

Problem Management: The Problem Management (PM) process includes the activities required to diagnose the root cause of incidents and determine a resolution to problems. It is responsible for managing the lifecycle of problems through investigation, documentation and eventual resolution.

Privileged User: User who by virtue of function is granted enhanced access privileges to the Solution in order to maintain it or perform administrative tasks. (e.g., System Administrators, Data Base Administrators, Information System Security Officer, etc.)

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 workflow diagram that depicts and models business processes that are performed by Users, roles or actors in an enterprise.

Production System: the complement of real-time and real-data IT systems that are running in production environment used within GC that will interoperate, communicate, execute programs or transfer data with the Solution in order to process CSP and CGP 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: Specific provisions of the *Access to Information Act* and the *Privacy Act* that apply to sensitive personal, private, and business information.

Protected A (low-sensitive): A type of information that, if compromised, could reasonably be expected to cause injury outside the National Interest, e.g., disclosure of exact salary figures.

Protected B (particularly sensitive): A type of information that, if compromised, could reasonably be expected to cause serious injury outside the National Interest, e.g., loss of reputation or competitive advantage.

Protected C (extremely sensitive): A type of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the National Interest, e.g., loss of life.

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.

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.

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.

Reliability: The measures expressed of the ability of a product to function successfully when required, for the period required, in the specified environment.

Simple Reliability (Reliability status): Type of security screening required before an employee can gain access to Protected A, B, or C information, assets or work sites. It is valid for 10 years

Release Management: Standardized methods and procedures for the integration and flow of development, testing, deployment, and support of the Solution.

Remote Access: Access to the ISS IT systems 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 Solution.

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

Root Cause Analysis: The activity using a wide range of approaches, tools, and techniques used to uncover causes of problems.

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.

Secure Access: The ability to permit or deny User access to resources within the Solution.

Secure Perimeter: Logical and physical boundary around network accessible resources and information, which is controlled and protected against unauthorized access from outside of the boundary.

Security Assessment: The on-going process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security. The Solution will be Security Assessed by the PWGSC IT Security Authority.

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. The Solution will be authorized by the PWGSC Chief Information Officer (CIO).

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.

Segregation of responsibilities: Security principle according to which responsibilities must be segregated when possible so that no one person has complete control over a particular resource or process. In some cases dual responsibility must be implemented so manipulation of a resource cannot be accomplished without the knowledge of another person.

Sensitive information: Classified or designated information.

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.

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 user 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.

Software Development Life Cycle (SDLC): The software development life cycle describe a process for planning, creating, testing, and deploying an information system.

System Administrator: A user role defined for the technical upkeep, configuration, and secure operation of the Solution.

System Development Life Cycle: Procedures documented and implemented to guide and control the design, development, approval, test, documentation, implementation, maintenance and protection of production software and data items.

T

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 application as well as the tools that support the IT Service.

Threat 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 to the Solution's Users.

Trainer: An individual who is responsible for teaching Users how to use the Solution.

Transport Layer Security and its predecessor, Secure Sockets Layer, both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP. Major websites use TLS to secure all communications between their servers and web browsers.

U

Unauthorized Access: When an entity gains unauthorized access to the Solution in order to commit another crime such as stealing or destroying information contained in the Solution (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 Solution

User Type	Examples
External User	**ISS clients:** Company Security Officers, Designated Officials, Authorized individuals, etc. ISS Partners: GS Security Officers, GC Procurement Officers, Foreign Security Officers, etc.
Internal User	**CSP/CGP Program Officers**: Registration Officers, Personnel Security Screening Officers, Inspectors, Investigators, etc.
Privileged User	System Administrators, Information System Security Officers, etc.

User Privilege: The authorization granted to a Solution user that enables her/him to access specific data/information and to perform specific actions. Example of privileges:

Privilege	**Description**
Create	Create a record
Read	View a record
Write	Make changes to a record
Delete	Delete a record
Append	Associate a record to another record
Append To	Associate entity record to this record
Assign	Transfer record ownership to another user
Share	Give access to a record to another user while keeping your own access
Re-parent	Assign a different parent to entity record

Users who have been delegated extra levels of control are called Privileged Users (e.g., System Administrators, ISSOs). Users who lack most privileges are defined as unprivileged, regular, or normal users.

User Profile: A record of User-specific data that defines the User's working environment and roles.

UTF: (UTF-8) is a character encoding capable of encoding all possible characters, or code points, defined by Unicode. The encoding is variable-length and uses 8-bit code units.

V

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.

X-Y-Z

ZIP folder: An electronic folder of compressed files.

APPENDIX 6 TO ANNEX A – ACRONYMS AND ABBREVIATIONS

APPENDIX 6 TO ANNEX A – ACRONYMS AND ABBREVIATIONS

This Appendix outlines acronyms and abbreviations that are employed throughout *ANNEX A – Statement of Work (SOW)*. This Appendix should be used in conjunction with *APPENDIX 5 to ANNEX A: Glossary of Terms*.

ACSO	Alternate Company Security Officer
AI	Authorized Individual
API	Application Programming Interface
BI	Business Intelligence
BPM	Business Process Management
CBSA	Canadian Border Services Agency
CGD	Controlled Goods Directorate
CGP	Controlled Goods Program
CGR	Controlled Goods Regulations
CIO	Chief Information Officer
CIOB	Chief Information Officer Branch
CISD	Canadian Industrial Security Directorate
CLF	Common Look and Feel
CMBP	Case Management and Best Practices
COMSEC	Communications Electronic Security
COSMIC	NATO Top Secret
COTS	Commercial-off-the-Shelf
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSE	Canadian Security Establishment
CSIS	Canadian Security Intelligence Service
CSO	Company Security Officer
CSP	Contract Security Program

DCN	(Fingerprint) Document Control Number
DND	Department of National Defence
DO	Designated Official
DOB	Departmental Oversight Branch
DOS	Designated Organisation Screening
DOCP	Designated Official Certification Program
DPA	Defence Production Act
DSA	Designated Security Authority
DSC	Document Safeguarding Capability
EA	Enhanced Access
ECL	Export Control List
ECM	External Credentials Management
EDI	Electronic Data Interchange
EPS	Electronic Procurement Solution
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
E-SRCL	Online Security Requirements Check List
ETL	Extract, Transform and Load
FA	Full Access
FAQ	Frequently Asked Questions
FIS	Facility Security Clearance Information Sheet
FISO	Field Industrial Security Officer
FSC	Facility Security Clearance
FISO	Field Inspector Security Officer
FSO	Foreign Security Officer
GAC	Global Affairs Canada

GC	Government of Canada
GC-SO	Government of Canada Security Officer
GC-PO	Government of Canada Procurement Officer
GCIP	Government of Canada Interoperability Platform
GISAB	Government Industrial Security Advisory Board
GUI	Graphical User Interface
HR	Human Resources
IAU	Investigations and Analysis Unit
ICAS	Internal Centralized Authentication Service
ICM	Internal Credential Management
IID	Inspections and Investigations Division
IISD	International Industrial Security Directorate
IM/IT	Information Management/Information Technology
IPC	Information Protection Center
ISM	Industrial Security Manual
ISMU	Industrial Security Memoranda of Understanding
ISP	Industrial Security Program
ISS	Industrial Security Sector
ISSO	Information System Security Officer
ISST	Industrial Security Systems Transformation
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITSG	Information Technology Security Guideline
JCO	US/Canada Joint Certification Office
JCP	US/Canada Joint Certification Program
KPI	Key Performance Indicator

KSO	Key Senior Official
LBA	Line of Business Access
LDAP	Lightweight Directory Access Protocol
LERC	Law Enforcement Record Check
MITS	Management of Information Technology Security
MOU	Memorandum of Understanding
MS	Microsoft
MSFT	Managed Secured File Transfer
NATO	North Atlantic Treaty Organisation
NCR	National Capital Region
NDA	Non-Disclosure Agreement
NNN	Non NATO National
NOS	NATO Office of Security
NPMS	National Project Management System
NSA	National Security Authority
OCC	Out of Country
OGD	Other Government Departments
OL	Official Languages
OLISS	Online Industrial Security Services
OPI	Office of Primary Interest
OS	Operating System
PA	Personnel Assigned
pdf	Portable Document Format
PGS	Policy on Government Security
PIPEDA	Personal Information Protection and Electronic Documents Act
PKI	Public Key Infrastructure

PML	Program Management and Learning
PMO	Project Management Office
PS	Professional Service
PSDCA	Personnel Screening Data Collection Automation System
PSOS	Private Security Organisation Screening
PSPC	Public Services and Procurement Canada
PSS	Personnel Security Screening
PSSD	Personnel Security Screening Division
PSSS	Personnel Security Screening Service (Online)
PWGSC	Public Works and Government Services Canada
RCMP	Royal Canadian Mounted Police
RFP	Request for Proposal
RFV	Request for Visit
RGBB	Receiver General Buy Button
ROD	Resolution of Doubt
ROW	Restricted to Own Work
RS	Reliability Status
SA&A	Security Assessment and Authorization
SaaS	Software as a Service
SC	Site Clearance
SCMS	Shared Case Management System
SDK	Software Developers Kit
SDLC	System Development Life Cycle
SDSD	Security Detailed Service Design
SHLSD	Security High Level Service Design
SI	Systems Integrator

SIEM	Security Information and Events Management
SIGINT	Signals Intelligence
SMS	Short Message Service
SaaS	Software as a Service
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SRCL	Security Requirements Checklist
SRTM	Security Requirements Traceability Matrix
SSC	Shared Services Canada
SSIU	Security Screening Investigation Unit
TBS	Treasury Board Secretariat
TLS	Transport Layer Security
TRA	Threat Risk Assessment
UAT	User Acceptance Test
USO	Unit Security Officer
VSC	Visit Security Clearance
WBS	Work Breakdown Structure
WF	Work Flow

ANNEX B – PRICE SCHEDULE

1. Instructions [These instructions will be removed at contract award and the Price Schedule will be renumbered accordingly.]**:**

1.1 The Bidder' is requested to submit along with its Financial Bid the completed Form 3 to Part 4 – Bid Solicitation – Financial Bid Form.
1.2 Bidders **should <u>not</u>** use the tables below in their Financial Bid.
1.3 The Contract Price Schedule will be developed based on inputs of the winning Bidder's Form 3 to Part 4 – Bid Solicitation – Financial Bid Form.

2. Introduction

The Contractor will be paid for work performed in accordance with the Basis of Payment of the Contract, pursuant to the firm price Work included in Sections 1, 2, 3, 4, 5, 6, 7 and 8 of ANNEX A – Statement of Work (SOW), and each approved Task Authorization. The estimates submitted with each Task Authorization must conform to article 7.2 - Task Authorization that will then be calculated in accordance with the rates in this ANNEX B.

3. Firm Lot Price – Sections 1, 2, 3, 4, 5, 6, 7, and 8 of ANNEX A - SOW

The Contractor will be paid a firm lot price for Work performed, in accordance with the Contract and Table 1 – Firm Lot Price and Milestone Schedule, below.

Table 1 - Firm Lot Price and Milestone Schedule			
(A) Milestone Description	**(B) Amount ($ CAD)**	**(C) Milestone Deliverables**	**(D) Delivery Due Date**
1	$0.00		
2	$0.00		
3	$0.00		
…	$0.00		
n	$0.00		
(E) Total Firm Lot Price [Sum of (B) for all Milestones, 1 through n]	**$0.00**		

The prices are in Canadian currency, Customs duties are included and Applicable Taxes are extra.

4. As-and-When-Requested Work

The Contractor will be paid in accordance with the firm all inclusive per diem rates in Table 2 for any Work performed pursuant to the Contract and any resulting Task Authorizations.

The rates are in Canadian currency, Customs duties are included and Applicable Taxes are extra.

Table 2 - As-and-When-Requested Work (Section 9 of ANNEX A - SOW) – Task Authorizations – Resource Categories		
Resource Categories	**Initial Contract Period** *(start/end dates to be inserted at award)* **Firm All-Inclusive Per Diem Rate (CDN $)**	**Option Periods 1, 2, 3, and 4** *(start/end dates to be inserted at award)* **Firm All-Inclusive Per Diem Rate (CDN $)**
Communications Consultant (Level 3)		
Courseware Developer (Level 3)		
Data Conversion Specialist (Level 3)		
Database Administrator (Level 3)		
Database Modeller (Level 3)		
Information Management Architect (Level 3)		
Programmer / Analyst – Business Objects (Level 3)		
Programmer / Analyst - MS Dynamics CRM (Level 3)		
Web Developer (Level 3)		

ANNEX C – SECURITY REQUIREMENTS CHECK LIST AND SECURITY CLASSIFICATION GUIDE

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EP243-17-0549 REVISED #1

Security Classification / Classification de sécurité

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 Services and Procurement Canada	Departmental Oversight Branch

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

Industrial Security Systems Transformation Project
The objective of this procurement is to acquire System Integration Services in support of project delivery

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No Non	☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No Non	☐ Yes Oui
6. Indicate the type of access required - Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non	☑ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p.ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No Non	☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciales **sans** entreposage de nuit?	☑ No Non	☐ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☑	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☑	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays : Restricted to Canada, including permanent residents	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☑	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☑	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EP243-17-0549 REVISED #1 MM

Security Classification / Classification de sécurité

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
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 :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets: ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

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 : See attached Personnel Security Specification Guide

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? ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted: ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

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? ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matérial PROTÉGÉ et/ou CLASSIFIÉ?

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? ☑ No / Non ☐ Yes / Oui
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?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EP243-17-0549 REVISED #17mm
Security Classification / Classification de sécurité

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).

SECURITY CLASSIFICATION GUIDE (SCG)

1) Reliability Status

The Contractor and/or any subcontractors must ensure that all contractor personnel working on Industrial Security Systems Transformation (ISST) project hold at minimum a valid Reliability status.

2) Secret Clearance

The Contractor and/or any subcontractors must ensure that all contractor personnel working on ISST project hold at minimum a valid Secret security clearance in order to have access to:

1) GC Production Data/Information;
2) GC Security Data/Information, including audit logs; and
3) GC Critical IT infrastructure, system(s) configuration including security components, and back-up media.

ANNEX D – NON-DISCLOSURE AGREEMENT

Non-Disclosure Agreement

I, _____, recognize that in the course of my work as an employee or subcontractor of _____, I may be given access to information by or on behalf of Canada in connection with the Work, pursuant to Contract Serial No. _____ between Her Majesty the Queen in right of Canada, represented by the Minister of Public Works and Government Services and _____ , including any information that is confidential or proprietary to third parties, and information conceived, developed or produced by the Contractor as part of the Work. For the purposes of this agreement, information includes but not limited to: any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form, recorded electronically, or otherwise and whether or not labeled as proprietary or sensitive, that is disclosed to a person or that a person becomes aware of during the performance of the Contract.

I agree that I will not reproduce, copy, use, divulge, release or disclose, in whole or in part, in whatever way or form any information described above to any person other than a person employed by Canada on a need to know basis. I undertake to safeguard the same and take all necessary and appropriate measures, including those set out in any written or oral instructions issued by Canada, to prevent the disclosure of or access to such information in contravention of this agreement.

I also acknowledge that any information provided to the Contractor by or on behalf of Canada must be used solely for the purpose of the Contract and must remain the property of Canada or a third party, as the case may be.

I agree that the obligation of this agreement will survive the completion of the Contract Serial No.: _____.

_____

Signature

_____

Date

ANNEX E – 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 resource categories defined in ANNEX A – Statement of Work, ANNEX F – Resource Category Information for Optional Services and the associated rates defined in ANNEX B – 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.

Industrial Security Systems Transformation (ISST)

Please provide the appropriate unique identification number and title:

Task Authorization (TA) Number

Title:_____

Approvals

	Name	Signature	Date
Initiated by:			
Approved by Project Authority:			
Approved by Contracting Authority:			
Accepted by Contractor:			

Remarks:

<Enter introductory remarks>

1 Instructions to the Contractor for TA Response:

Whether the TA request is solution based or resource based, the Contractor must substantiate all costs by providing a price breakdown, and where applicable, by identifying the proposed resource categories and All Inclusive Per-Diem Rates in accordance with ANNEX F – Resource Category Information for Optional Services and ANNEX B – Price Schedule, respectively.

2 Background Information

<Enter background information.>

3 Overview of Requirement

<Provide a high level description of requirement and indicate the labour category.>

4 Objective and Scope

<Define the objectives and scope of this TA.>

5 Detailed Requirements

<Provide a description of the requirements that will be addressed by this TA. Including security clearance and language requirements that align with the Contract, as well as requirements that are within scope of the resource category descriptions and minimum mandatory qualifications in ANNEX F. >

6 Project Plan

<Provide a high level plan outlining the project steps, timelines, resource requirements and interdependencies.>

7 Roles and Responsibilities

<Identify the roles and responsibilities associated with this TA.>

8 Project Deliverables and Milestones

<Provide a description of the project deliverables and identify major milestones with dates.>

9 Assumptions and Constraints

<Detail any assumptions and constraints associated with the completion of this TA.>

10 Basis of Payment and Cost Detail

<Provide the basis of payment and detailed costing to support justification for this TA.>

11 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.>

ANNEX F – RESOURCE CATEGORY INFORMATION FOR OPTIONAL SERVICES

1. General Considerations

The purpose of this annex is to describe the responsibilities and minimum mandatory qualifications and expertise for the different Professional Services resource categories which may be required on an "as-and-when requested" basis, in accordance with the Contract and Task Authorizations, ANNEX A – Statement of Work, and ANNEX B – Price Schedule.

The following resource categories may be requested and are subject to minimum mandatory qualifications:

(a) Communications Consultant (Level 3);
(b) Courseware Developer (Level 3);
(c) Data Conversion Specialist (Level 3);
(d) Database Administrator (Level 3);
(e) Database Modeller (Level 3);
(f) Information Management (IM) Architect (Level 3);
(g) Programmer / Analyst – Business Objects (Level 3);
(h) Programmer / Analyst - MS Dynamics CRM (Level 3); and
(i) Web Developer (Level 3).

Additional resource categories may be identified and requested during the performance of the Contract. The responsibilities and minimum mandatory qualifications and expertise for the additional Professional Services resource categories will be developed. The additional resource categories are subject to the minimum mandatory qualifications.

2. Résumés for Proposed Resources in response to Task Authorizations:

Unless specified otherwise in the Contract, the Contractor's response to a TA or TA revision must include résumés for the proposed resources that demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to résumés and resources:

(a) Proposed resources may be employees of the Contractor or employees of a subcontractor, or these individuals may be independent contractors to whom the Contractor would subcontract a portion of the Work.

(b) For educational requirements for a particular degree, designation or certificate, only consider educational programmes that were successfully completed by the resource by the time of TA response submission will be considered.

(c) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of TA response submission and must continue, where applicable, to be a member in good standing of the profession's governing body throughout the period of the TA.

(d) The Contractor is requested to provide complete details as to where, when, month and year, and how, through which activities/responsibilities, the stated qualifications/experience were obtained.

(e) Canada may request proof of successful completion of formal training, as well as reference information. Canada may conduct reference checks to verify the accuracy of the information provided. If reference checks are done, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will not consider a mandatory criterion met unless the response is received within 5 working days. On the third working day after sending out the e-mails, if Canada has not received a response, Canada will notify the Contractor by e-mail, to allow the Contractor to contact its reference directly to ensure that it responds to Canada within 5 working days. Wherever information provided by a reference differs from the information supplied by the Contractor, the information supplied by the reference will be the information assessed. A mandatory criteria will not be considered as met if the reference customer is not a customer of the Contractor itself (for example, the customer cannot be the customer of an affiliate of the Contractor). Nor a mandatory criteria will be considered as met if the customer is

itself an affiliate or other entity that does not deal at arm's length with the Contractor. Crown references will be accepted.

(f) During the assessment of the resources proposed, should the references for two or more resources required under that TA either be unavailable or fail to substantiate the required qualifications of the proposed resources to perform the required services, the Contracting Authority may find the quotation to be non-responsive.

3. Required Services and Requirements for Task Authorizations

3.1 Communications Consultant (Level 3)

3.1.1 Required Services

The required services may include, but are not limited to the following:

(a) Planning, researching, modifying, assisting, writing and/or reviewing memos, scripts, plays, essays, speeches, manuals and other non-journalistic articles with conformance to established standards;
(b) Developing and implementing strategic communication plans in geographically dispersed organizations going through an organizational transformation (change management);
(c) Providing communications consultation advice to support strategic communications initiatives and strategies;
(d) Creating communications support materials;
(e) Developing and implementing creative communication and information products using a variety of tools, techniques and media and selecting an appropriate medium to convey information, ideas, and results;
(f) Developing and implementing communication strategies and plans;
(g) Expressing and exchanging information in a clear and concise manner;
(h) Ensuring information is communicated to the appropriate people in a timely manner;
(i) Preparing reports for specific purposes using clear, communicative, and professional language (e.g., audit reports, management letters, consulting reports, financial reports);
(j) Ensuring communications are clearly understood by encouraging and listening to feedback both internally and externally in the organization;
(k) Structuring external communications to project an appropriate corporate image;
(l) Ensuring confidentiality with respect to organizational or client information and data.
(m) Determining target audiences in order to better develop messages;
(n) Identifying and determining communications impediments and barriers;
(o) Providing advice on matters relating to policy/program development approaches or options and communications planning alternatives (internal or external);
(p) Researching, developing and implementing communications strategies involving social media and related content (i.e. blogs, microblogs, wikis, crowdsourcing, content communities, social networks, etc);
(q) Providing support and assisting communicators in using social media channels to complement traditional channels; and
(r) Providing suggestions on cost-cutting measures in the communications process.

3.1.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Communications Consultant.
M2	Must possess a University degree or a College diploma (in any field).
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (c), (d), (e), (f), (h), (m), (n) and (o) of 3.1.1.

3.2 Courseware Developer (Level 3)

3.2.1 Required Services

The required services may include, but are not limited to the following:

(a) Perform needs assessment/analysis for training purposes;
(b) Plan and monitor training projects;
(c) Perform job, task, and/or content analysis;
(d) Write criterion-referenced, performance-based objectives;
(e) Recommend instructional media and strategies;
(f) Develop performance measurement standards;
(g) Develop training materials;
(h) Prepare end-users for implementation of courseware materials; and
(i) Communicate effectively by visual, oral, and written form with individuals, small groups, and in front of large audiences.

3.2.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Courseware Developer.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (c), (e), (g) and (h) of 3.2.1.

3.3 Data Conversion Specialist (Level 3)

3.3.1 Required Services

The required services may include, but are not limited to the following:

(a) Oversee all facilities of the conversion process;
(b) Complete mapping, interfaces, mock conversion work, enhancements, actual conversion, and verify completeness and accuracy of converted data;
(c) Establish a strong working relationship with all clients, interact effectively with all levels of client personnel, and provide conversion support;
(d) Analyze and coordinate data file conversions; and
(e) Work with importing files from heterogeneous platforms.

3.3.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Data Conversion Specialist.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (d) and (e) of 3.3.1.

3.4 Database Administrator (Level 3)

3.4.1 Required Services

The required services may include, but are not limited to the following:

(a) Customize database conversion routines;
(b) Finalize Conversion Strategy;
(c) Generate new database with the client;
(d) Maintain data dictionaries;
(e) Develop and implement procedures that will ensure the accuracy, completeness, and timeliness of data stored in the database;
(f) Develop and implement security procedures for the database, including access and user account management;
(g) Maintain configuration control of the database;
(h) Perform and/or coordinate updates to the database design;
(i) Control and coordinate changes to the database, including the deletion of records, changes to the existing records, and additions to the database;
(j) Develop and coordinate back-up, disaster recovery and virus protection procedures; and
(k) Advise programmers, analysts, and users about the efficient use of data.

3.4.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Database Administrator.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (e), (f), (h) and (j) of 3.4.1.

3.5 Database Modeller (Level 3)

3.5.1 Required Services

The Database Modeller has both strategic and tactical responsibility for developing and maintaining the Architecture and Data Models for corporate and project specific initiatives. This responsibility includes the identification of data most valuable to the department, the integration of this data, and the development of core relating data models. The resulting data models will be based on data architecture and modeling design principles and tenets.

The required services may include, but are not limited to the following:

(a) Design, develop and maintain Logical Data Models;
(b) Analyze proposed changes to databases from the context of the Logical Data Model;
(c) Provide technical expertise in the use and optimization of data modeling techniques to team members;
(d) Provide technical assistance, guidance and direction in terms of data analysis and modeling to team members;
(e) Provide assistance to project team and business users relating to data issues and data analysis concepts;
(f) Participate in the development of data modeling and metadata policies and procedures;
(g) Participate in data analysis as a result of new/updated requirements;
(h) Apply approved changes to logical data models;
(i) Comply with corporate data architectures, strategies and frameworks, including enterprise data warehouse activities;
(j) Analyze and evaluate alternative data architecture solutions to meet business problems/requirements to be incorporated into the corporate data architecture;
(k) Review corporate architecture strategies and directions, data requirements, and business information needs and devise data structures to support them;
(l) Improve modeling efficiency through recommendations on how to better utilize current metadata repositories;

(m) Comply with corporate repository metadata directions;
(n) Provide input to refinement of data architectures;
(o) Participate in data architecture refinement;
(p) Define access strategies; and
(q) Construct, monitor and report on work plans and schedules.

3.5.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Database Modeller.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (c), (d), (e), (g), (i) and (j) of 3.5.1.

3.6 Information Management (IM) Architect (Level 3)

3.6.1 Required Services

The required services may include, but are not limited to the following:

(a) Analyse existing capabilities and requirements, develop redesigned frameworks and recommend areas for improved capability and integration;
(b) Develop and document detailed statements of requirements;
(c) Evaluate existing procedures and methods, identify and document database content, structure, and application subsystems, and develop data dictionary;
(d) Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems;
(e) Prototype potential solutions, provide trade-off information and suggest recommended courses of action;
(f) Perform information modelling in support of BPR implementation;
(g) Perform cost/benefit analysis of implementing new processes and solutions;
(h) Provide advice in developing and integrating process and information models between business processes to eliminate information and process redundancies; and
(i) Provide advice in defining new requirements and opportunities for applying efficient and effective solutions; identify and provide preliminary costs of potential options.

3.6.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as an IM Architect.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (d) and (h) of 3.6.1.

3.7 Programmer/Analyst (Level 3) – Business Objects

3.7.1 Required Services

The required services may include, but are not limited to the following:

(a) Create and modify code and software;
(b) Create and modify screens and reports;

(c) Gather and analyze data for the conduct of studies to establish the technical and economic feasibility of proposed computer systems, and for the development of functional and system design specifications;
(d) Design methods and procedures for small computer systems, and sub-system of larger systems;
(e) Develop, test and implement small computer systems, and sub-systems of larger systems; and
(f) Produce forms, manuals, programs, data files, and procedures for systems and/or applications.

3.7.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Programmer / Analyst.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (c), (d), and (e) of 3.7.1.
M4	Must have a minimum of three (3) years of experience, within the last ten (10) years, developing business intelligence reporting using SAP Business Objects.

3.8 Programmer/Analyst (Level 3) – MS Dynamics CRM

3.8.1 Required Services

The required services may include, but are not limited to the following:

(a) Create and modify code and software;
(b) Create and modify screens and reports;
(c) Gather and analyze data for the conduct of studies to establish the technical and economic feasibility of proposed computer systems, and for the development of functional and system design specifications;
(d) Design methods and procedures for small computer systems, and sub-system of larger systems;
(e) Develop, test and implement small computer systems, and sub-systems of larger systems; and
(f) Produce forms, manuals, programs, data files, and procedures for systems and/or applications.

3.8.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Programmer/Analyst.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (c), (d), and (e) of 3.8.1.
M4	Must have a minimum of three (3) years of experience, within the last ten (10) years, designing, developing and implementing systems using MS Dynamics CRM.

3.9 Web Developer (Level 3)

3.9.1 Required Services

The required services may include, but are not limited to the following:

(a) Develop and prepare diagrammatic plans for web based service delivery over the internet;
(b) 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;
(c) 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;
(d) Design high-usability web pages to meet the requirement;

(e) Verify accuracy and completeness of programs by preparing sample data, and testing them by means of system acceptance test runs made by operating personnel;
(f) Correct program errors by revising instructions or altering the sequence of operations; and
(g) Produce test instructions, and assemble specifications, flow charts, diagrams, layouts, programming and operating instructions to document applications for later modification or reference.

3.9.2 Minimum Mandatory Qualifications

No.	Description of Criteria
M1	Must have a minimum of ten (10) years of experience as a Web Developer.
M2	Must possess a University degree or a College diploma in a related field.
M3	Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b), (c), and (d) of 3.9.1.
M4	Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery using Adxstudio Portals.

ATTACHMENT 1 TO PART 4 – TECHNICAL EVALUATION

1. OVERVIEW OF THE TECHNICAL EVALUATION

This attachment outlines the evaluation methodology to be used in the evaluation of proposals received in response to this RFP. The evaluation methodology is structured to ensure transparent and consistent assessment of Bidders' Technical Proposals. The Bidder's Technical Proposal must respond to each of the mandatory criteria and should respond to each of the point rated criteria in sufficient depth to permit the evaluation team to evaluate its compliance or to score the response, as applicable, in accordance with the stated criteria. The Bidder is requested to provide any information that it considers pertinent to support the evaluation of the response to an individual requirement.

Technical Evaluation Summary			
ID	**Mandatory Criteria**		**Met/Not Met**
M1	Corporate Reference Projects: Business Process Re-engineering and Change Management		
M2	Corporate Reference Projects: IT Solution		
M3	Customer References		
ID	**Point Rated Criteria**	**Maximum Points**	**Actual Score**
R1	Project Management	620	
R2	Business Process Re-engineering	360	
R3	Relationship Management	170	
R4	Security Management	360	
R5	Sensitive Data Migration	200	
R6	Change Management Plan	380	
R7	Testing Plan	170	
R8	Corporate Reference Projects: Government of Canada Client	80	
R9	Corporate Reference Projects: Case Management and Microsoft Dynamics CRM	160	
Maximum Total Points for Point Rated Criteria		**2500**	
Minimum Pass Mark for Point Ra80ted Criteria (70%)		**1750**	

Notes: *Refer to the Generic Technical Evaluation Scale included at section 3 of this attachment, for further details regarding scoring methodology of the point rated criteria.*

2. EVALUATION OF EXPERIENCE OF BIDDER'S TEAM MEMBERS

a. For the purposes of the mandatory technical criteria M1 & M2, under section 3. Mandatory Technical Criteria, and the point-rated criteria R8 & R9, 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, R8 and R9. 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 Sub-Form 5 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 CRITERIA

Each Bid will be evaluated for compliance with the following mandatory criteria. Bids which fail to meet the mandatory criteria will be declared non-responsive and will not be considered further. The Bidder is requested to provide the necessary documentation to support compliance. Each mandatory criterion should be addressed separately. For clarity, for the purposes of this evaluation, a project is considered to have been successfully delivered when the Customer Reference confirms that the services contracted for were delivered within the mutually agreed upon work requirements, price, schedule, and service levels/performance agreement.

ID	Mandatory Requirement	Cross Reference to Bidder's Proposal
M1	**Corporate Reference Projects: Business Process Re-Engineering and Change Management** The Bidder must provide **three (3)** Reference Projects similar to that of ANNEX A, Sections 2 through 7, completed within **fifteen (15)** years of the date of Bid Closing and have a public-facing internet-based information exchange component. For <u>all</u> Reference Projects the Bidder must have been contracted to provide services including Business Process Re-engineering and Change Management for a business systems transformation project, from high level business requirements through to an operational, Customer accepted solution. For the purpose of this evaluation, a similar project would be defined as no less than 35% of the number of users, number of accounts, and number and diversity of transactions indicated in ANNEX A, Section 1, 3.1, Volumetric Data. A. One (1) of the three (3) Reference Projects must emphasize all of the following elements of Change Management: i. Developing a change management approach ii. Developing a communication plan iii. Delivering communication plan iv. Developing a training plan v. Delivering a training plan B. One (1) of the three (3) Reference Projects must emphasize all of the following elements of Business Process Re-engineering: i. Developing a business process re-engineering plan ii. Recommending options for business process optimization iii. Implementing business process re-engineering plan C. For at least one (1) Reference Project, the Reference Project must have been initiated and completed within five (5) years of the date of Bid Closing. For each Reference Project, the Bidder must : D. Provide a detailed description, including but not limited to the following: i. Executive Summary; ii. Problem statement; iii. Project Management Strategy that includes at a minimum: a. Industry standard, best practice or corporate methodology used; b. Implementation strategy;	

	c. Problem/Issue management; d. Communications management; e. Risk mitigation; f. Technologies used or implemented; g. Resource management; h. Project schedule management (including project timeline, from inception to completion); iv. Budget management (including the overall cost of services contracted for both at contract award and at project closeout); v. Description of users; vi. Volumetrics, including number of internal users, number of transactional requests, and diversity of transactions; and vii. Contract Disputes and Performance Issues.	
M2	**Corporate Reference Projects: IT Solution** The Bidder must provide **three (3)** Reference Projects similar to that of ANNEX A, Sections 2 through 7, completed within **fifteen (15)** years of the date of Bid Closing and have a public-facing internet-based information exchange component. For <u>all</u> Reference Projects, the Bidder must have been contracted to provide three (3) of the six (6) key activities (IT design, configuration, development, implementation, integration and data migration services). All six (6) key activities must have been a contracted service at least once, Reference Project. For the purpose of this evaluation, a similar project would be defined as no less than 35% of the volumetric data indicated in ANNEX A, Section 1, 3.1, Volumetric Data. Specifically; number of users, number of accounts, and number and diversity of transactions. For each Reference Project, the Bidder must: A. Provide a detailed description, including but not limited to the following: i. Executive Summary; ii. Problem statement; iii. Project Management Strategy that includes at a minimum: a. Industry standard, best practice or corporate methodology used; b. Implementation strategy; c. Problem/Issue management; d. Communications management; e. Risk mitigation; f. Technologies used or implemented; g. Resource management; h. Project schedule management (including project timeline, from inception to completion); iv. Budget management (including the overall cost of services contracted for, both at contract award and at contract closeout); v. Description of users; vi. Volumetrics, including number of internal users, number of transactional requests, and diversity of transactions; and Contract Disputes and Performance Issues. <u>In addition, the Bidder must demonstrate that the following requirements are satisfied collectively by the three (3) Reference Projects submitted:</u> B. For at least (1) Reference Project, the value of the professional services provided must have been $10M ($CDN, taxes excluded) or greater within a single contract. For evaluation purposes, the exchange rate used for currency adjustment will be the annual average exchange rate, as published by the Bank of Canada, determined by the year that the contract was awarded to the Bidder for the Reference Project. C. For at least one (1) Reference Project, the following four (4) key activities (IT design, implementation, integration and data migration services) and one of the following two (2): (configuration or development) must have been provided within a single contract. D. For at least one (1) Reference Project, the solution must have been a business systems transformation project for a government entity (federal, provincial, or municipal levels of government).	

	E. For at least one (1) Reference Project, the solution implemented must have had security requirements to those identified in ANNEX A, Section 5, 1.2. IT Security Requirements. F. For at least one (1) Reference Project, the Reference Project must have been initiated and completed within five (5) years of the date of Bid Closing.	
M3	**Customer References** For each Reference Project submitted for M1 and M2, the Bidder must provide a Customer Reference with accurate contact information. The Customer Reference will be contacted to validate the information provided in the Bidder's response, in accordance with the reference check process described in Part 4.2 (d).	

3. POINT RATED CRITERIA

Bids which meet all the mandatory criteria will be evaluated and scored as specified in the scale and table below and the scoring grid in section 1 – "Overview of the Technical Evaluation". Bids which fail to meet the overall minimum pass mark for the point rated criteria will be declared non-responsive and will not be considered further. The Bidder is requested to provide the necessary documentation to support compliance. Each point rated criterion should be addressed separately. The successful Bidder will be expected to utilize the procedures/methodologies described within its bid in the various requested documents, using them as a basis for solution delivery upon contract award.

Generic Scale	
0%	**No Response** – The Bidder either did not respond or the information submitted was not at all relevant to the criterion.
30%	**Partial Response** – The information provided did not respond to most of the requirements of the rated criterion, or has significant weaknesses. The Bid demonstrates little understanding of the solicitation requirements. The proposed approach does not address important factors and minimally demonstrates technical/business value to Canada.
60%	**Fair Response** – The information provided responds to some of the requirements of the rated criterion, but there are quite a few noticeable weaknesses. The Bid demonstrates some understanding of the solicitation requirements. The proposed approach fairly addresses important factors and demonstrates good technical/business value to Canada.
80%	**Satisfactory Response** – The information provided responds to most of the requirements of the rated criterion very well. The Bid demonstrates adequate understanding of the solicitation requirements. The proposed approach has few noticeable weaknesses and provides great technical/business value to Canada.
100%	**Excellent Response** – The information provided responds to all of the requirements of the rated criterion very well. The Bid demonstrates an in-depth and comprehensive understanding of the solicitation requirements. The proposed approach addresses all important factors, has no noticeable weaknesses and provides excellent technical/business value to Canada.

For each Criterion, Bidders' scores will be distributed as follows:
0% – receives 0% of the points assigned to a criterion
30% – receives 30% of the points assigned to a criterion
60% – receives 60% of the points assigned to a criterion
80% – receives 80% of the points assigned to a criterion
100% – receives 100% of the points assigned to a criterion

For example, if a Bid obtains 80% in the evaluation of R1, then the Bidder's score for that criterion would be calculated as follows:

Score for R1:

Maximum Available Points of Criterion R1 – Project Management = 620 points

80% x 620 points = 496 points

ID	Point Rated Criteria	Maximum Available Points	Cross Reference to Bidder's Proposal
R1	**Project Management** The Bidder should provide a Preliminary Project Management Plan that reflects the Bidder's strategy to successfully implement the requirements described in ANNEX A, Section 2 to 7; The plan must align to the National Project Management System (NPMS) framework. Canada will evaluate the Bidder's proposed Project Management Plan based on the degree to which it responds to the following requested elements and how they support the intended outcomes listed in ANNEX A, Section 1 and 7: A. **Project Governance and Team Structure Document**, including the following: i. Roles and responsibilities matrix including the Contractor and GC; ii. Description of the high-level project team structure and relationships (highlighting groups and entities that form the project team); and iii. Diagram of the governance model that will be employed by the Bidder for this project. B. **Scope Management Plan** describing how scope will be managed throughout the Project Delivery Stage. This narrative should address the following: i. A Project Scope Statement outlining the Bidder's understanding of the project scope, major deliverables and proposed acceptance criteria, as well as constraints and assumptions; and ii. A description of how scope will be managed throughout the Project Delivery Stage. This must include information on specific scope management processes such as scope verification and control, development of Work Breakdown Structure (WBS), roles and responsibilities, tools, techniques and reporting. C. **Schedule Management Plan** that outlines the Bidder's strategy for managing ISST project activities. The response should contain the following: i. For each project activity and milestone, the associated deliverables including the critical path used to achieve said deliverables; ii. Mitigation measures and strategies to handle schedule deviations. D. **Project Schedule** that outlines the activities and timelines for the project. The response should contain the following: i. WBS denomination at [minimum] 2 levels (in addition	**Maximum Points: 620** Part A : Maximum Points : 60 i. Maximum Points: 20 ii. Maximum Points: 20 iii. Maximum Points: 20 Part B Maximum Points: 140 i. Maximum Points: 70 ii. Maximum Points: 70 Part C Maximum Points:80 i. Maximum Points: 45 ii. Maximum Points: 35 Part D Maximum Points: 70 i. Maximum	

	to the project context): The WBS should identify all major work packages required to deliver the project; ii. Estimated duration for each activity, and dependencies (predecessors); The Project Schedule is requested to be delivered in MS Project 2013 or higher and must address the constraints identified throughout ANNEX A. The schedule must assume a start date of September 1, 2017 and respect a production launch date of March 31, 2019. E. **Risk Management Plan**, in alignment with NPMS that includes the following: i. A description of the process for identifying, analyzing, and prioritizing project risks; ii. The methods that will be used to track risks, evaluate changes in individual risk exposures, and respond to those changes; iii. Risk management roles and responsibilities; and iv. A list of five (5) project risks and proposed mitigation strategies. F. **Quality Management Plan** that outlines the Bidder's strategy to ensure that quality is integrated into project management and product development, deliverables and processes, from both a business process and solution implementation perspective. The response should contain the following: i. A description of the processes for Quality Planning, Quality Assurance and Quality Control; ii. Methods, tools and techniques that will be used for Quality Management; iii. Quality Management roles and responsibilities; iv. Outline an approach to address quality non-compliance.	Points: 35 ii. Maximum Points: 35 Part E Maximum Points: 150 i. Maximum Points: 30 ii. Maximum Points: 40 iii. Maximum Points: 30 iv. Maximum Points: 50 Part F Maximum Points : 120 i. Maximum Points : 40 ii. Maximum Points : 30 iii. Maximum Points: 30 iv. Maximum Points: 20	
R2	**Business Process Re-engineering** The Bidder should provide a preliminary Business Process Re-engineering strategy. Canada will evaluate the degree to which the Bidder's preliminary Business Process Re-engineering strategy meets the benefits identified in ANNEX A, Section 2, 1.1 and demonstrates: A. An understanding of the current ISS business processes and the need for security practices within the various business operations; B. A plan to conduct a business process gap analysis; C. An understanding of constraints and impacts; D. Four examples of opportunities to improve process efficiency and effectiveness and proposed implementation approaches; E. An understanding of risks and options for risk resolution or mitigation; and F. Scheduling of business process re-engineering activities.	**Maximum Points: 360** Part A Maximum Points: 60 Part B Maximum Points: 50 Part C Maximum Points: 40 Part D Maximum Points: 60 (Maximum 15 points for each element) Part E Maximum Points: 50 Part F Maximum Points: 100	
R3	**Relationship Management** The Bidder should describe their approach to Relationship Management. Canada will evaluate the degree to which the Bidder's response considers the following elements:	**Maximum Points : 170** Part A Maximum	

	A. Overall approach to Government of Canada and Systems Integrator relationship management; B. Communications between the Government of Canada and the Systems Integrator in respect to a proposed governance model and team structure as detailed in R1. A.; C. Issue management and resolution; D. Joint planning and managing of changes to project scope and schedule.	Points : 50 Part B Maximum Points : 30 Part C Maximum Points: 40 Part D Maximum Points : 50	
R4	**Security Management** The Bidder should provide a Concept of Security Operations document which describes an operational scenario for the ISST solution. The response should contain sufficient information to be considered an end to end description. The document should highlight the requirements for security as indicated in the Security Requirements section of ANNEX A, Section 4. Canada will evaluate the degree to which the Bidder's approach to Security management reflects the required security controls. In particular, the approach should : A. Contain a high level, end to end description of security operations; B. Reference and address all parts of SC-01 Access Control and Account Management; C. Reference and address all parts of SC-04 Audit and Accountability; and D. Reference and address all parts of SC-07 Identification and Authentication within the Security Operations document.	**Maximum Points : 360** Part A Maximum Points : 120 Part B Maximum Points : 80 Part C Maximum Points: 80 Part D Maximum Points : 80	
R5	**Sensitive Data Migration** Based on its previous IT integration project experience, the Bidder should describe its approach to the data migration requirement for this solicitation. (For volumetrics, refer to Section 1, Item 3.1 of ANNEX A) Canada will evaluate the degree to which the Bidder's approach demonstrates an understanding of the data migration activity required for this project. Specifically, the approach should address: A. An approach to data migration listing key activities to be undertaken; B. The defined roles, responsibilities, and expectations of the Bidder and Canada; C. The risks and mitigation strategies specifically related to migration activities; D. Activities during data migration which will help satisfy the ITSG-33 based security requirements located within the Security Requirements table, specifically: i. SC-21 Protection of Information; ii. SC-23 Information System Monitoring; iii. SC-28 Information System Recovery and Reconstitution; and iv. SC-31 Information Input Validation. v. SC-44 Security - General	**Maximum Points: 200** Part A Maximum Points: 70 Part B Maximum Points: 40 Part C Maximum Points: 40 Part D Maximum Points: 50 (Maximum 10 points for each element)	
R6	**Change Management Plan** The Bidder should provide a Preliminary Change Management Plan to describe the methods, approaches, tools and resources it will employ to address the Change Management requirements of this solicitation. Canada will evaluate the degree to which the Bidder's Preliminary Change Management Plan supports the successful transition from "as-	**Maximum Points: 380**	

	is" to "to be" states and demonstrates: A. A comprehensive understanding of the Change Management requirements; B. Consideration of the following: i. Avoidance of disruption of service to Canadians; ii. Facilitation of the adoption of process and terminology transitions for all end users, including external users and internal staff; iii. Appropriate, accurate and timely use and input to the new system; and iv. The quality and integrity of the services rendered. C. A comprehensive evaluation method for assessing effectiveness of change management activities.	Part A Maximum Points: 100 Part B Maximum Points: 200 i. Maximum Points: 50 ii. Maximum Points: 50 iii. Maximum Points: 50 iv. Maximum Points: 50 Part C Maximum Points: 80	
R7	**Testing Plan** The Bidder should prepare a preliminary testing plan in accordance with the requirements of the ANNEX A, Section 6. The Bidder should be guided by the business and technical requirements and conceptual architecture for preparing the test plan. Canada will evaluate the degree to which the Bidder's test plan demonstrates: A. Due consideration of related Security requirements from SC-42 Security Integration Test Plan as well as Section 6 of ANNEX A; B. Adequate test coverage to ensure Solution go-live readiness. Due consideration of and reference to : i. Integration testing; ii. Functional and non-functional Testing, including Security Testing; iii. Data Validation Testing; iv. Client acceptance testing. C. The identification of risk and its management.	**Maximum Points: 170** Part A Maximum Points: 40 Part B Maximum Points: 100 (Maximum 25 points for each element) Part C Maximum Points: 30	
R8	**Corporate Reference Projects: Government of Canada Client** The Bidder should demonstrate, for at least one (1) and up to three (3) of the Reference Projects provided in response to **Mandatory Requirement M2,** that it has successfully delivered a solution similar in nature and scope to that described in Annex A, Section 2 to 7, for a Government of Canada client.	**Maximum Points: 80** One (1) Reference Project: 30 Two (2) Reference Projects: 50 Three (3) Reference Projects: 80	
R9	**Corporate Reference Projects: Case Management and Microsoft Dynamics Client Relationship Management** The Bidder should demonstrate: A. At least one (1) of the three (3) of the Reference Projects provided in response to Mandatory Requirement M2, that it has successfully delivered a solution, requiring both IT design and configuration, using a Case Management solution. B. If the Bidder demonstrates that it has used a Case Management solution and Microsoft Dynamics CRM for the same Reference Project, that Project will count as two Reference Projects.	**Maximum Points: 160** Maximum Points for A: 80 One (1) Reference Project: 30 Two (2) Reference	

	For the purposes of this evaluation, Case Management is defined as the management of activities including but not limited to; the initiation, coordination, research, maintenance and completion of a service request action from a client, until its resolution.	Projects: 50 Three (3) Reference Projects: 80 Maximum Points for B: 80 One (1) Reference Project: 30 Two (2) Reference Projects: 50 Three (3) Reference Projects: 80	

FORM 1 TO PART 4 - RFP SUBMISSION FORM

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the bid submission date. 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.

Sub-form 1A: Bidder's Information

#	Bidder's Information
	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 complete section (d) below. [*Bidder to add more rows if more than one joint venture member*]	
(d)	Joint venture member full legal name:
	Joint venture member address:
RFP Submission Requirements It is the Bidder's sole responsibility to ensure its response addresses all requirements outlined in the RFP.	

Sub-form 1B: Bidder's Authorization

Bidder's 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.	
(e)	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 (f) below. [*Bidder to add more rows if more than one joint venture member*]	
(f)	Name:
	Address:
	Email:
	Signature of authorized representative of Bidder:
	Phone:
	Date:

Sub-form 2: Former Public Servant

<table>
<tr><td rowspan="2">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>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>Name(s) of former public servant:</td></tr>
</table>

Sub-form 3: Work Force Adjustment

<table>
<tr><td rowspan="9">Work Force Adjustment Directive
See Sub-form 2 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.</td><td colspan="2">Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive?

Yes ☐ No ☐</td></tr>
<tr><td colspan="2">If yes, provide the following information:</td></tr>
<tr><td>a. name of former public servant;</td><td></td></tr>
<tr><td>b. conditions of the lump sum payment incentive;</td><td></td></tr>
<tr><td>c. date of termination of employment;</td><td></td></tr>
<tr><td>d. amount of lump sum payment;</td><td></td></tr>
<tr><td>e. rate of pay on which lump sum payment is based;</td><td></td></tr>
<tr><td>f. period of lump sum payment including start date, end date and number of weeks; and</td><td></td></tr>
<tr><td>g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.</td><td></td></tr>
</table>

Sub-form 4: Federal Contractors Program for Employment Equity

For further information on the Federal Contractors Program for Employment Equity visit https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html.

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).

Sub-form 5: Team Certification

The Bidder must certify that it meets the following mandatory requirements otherwise its bid will be declared non-responsive:

(i) The Bidder must identify and provide all its Team Members in the bid and have signed formal Teaming Agreement(s) or signed Contract(s) 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) The Bidder must obtain the permission from the Team Members to use their service experience in response to the RFP requirements;

(iii) Where the Team Member is a related organization (i.e. parent, affiliated and/or subsidiary organization), the Teaming Agreement(s) or Contract(s) 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;

(iv) 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, and

(v) 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.

If the Bidder is awarded a Contract, and for reasons beyond its control, the Team Member of the Bidder is unable to provide the services to which the experience relates and which was used to meet evaluation criteria of the RFP, the Bidder may propose a substitute with equivalent or better qualifications and experience. The Bidder must advise the Contracting Authority within 15 business days 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. If the Bidder cannot provide a satisfactory substitute for the original proposed Team Member, Canada may terminate the Contract for default.

For greater clarity, the following situations may be considered as beyond the control of the Bidder: death, sickness, retirement, resignation, dismissal for cause or termination of an agreement for default of critical corporate resources that would prevent the Team Member from delivering services under the Contract; or where the Team Member is bankrupt or, for whatever reason, its activities are rendered inoperable for an extended period; or a merger or acquisition of the Team Member.

The Bidder hereby certifies compliance with the above noted requirements and has 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).

The Bidder also certifies that it has permission from the team members named above to propose their services in relation to the work to be performed.

FORM 2 TO PART 4 – PROJECT REFERENCE CHECK FORM

PROJECT REFERENCE CHECK FORM

Instructions to Bidders:

a) In accordance with *Part 4 Evaluation Procedures and Basis of Selection, 4.2.4 Reference Checks*, Bidders are requested to submit a Project Reference Check Form for each of the projects identified in Attachment 1 to Part 4 – Technical Evaluation of the RFP.

b) 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.

c) Canada may contact the client contact, provided for the referenced project, to validate the information provided.

#	Response		
(a)	Evaluation Criteria Number (from Attachment 1 to Part 4 – Technical Evaluation)		
(b)	Bidder's Full Legal Name and Full Legal Name of Bidder's Team Member whose experience is being used to meet the evaluation criteria, if applicable (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		

FORMULAIRE 3 DE LA PARTIE 4 – DEMANDE DE SOUMISSION – FORMULAIRE DE SOUMISSION FINANCIÈRE

FORM 3 TO PART 4
BID SOLICITATION - FINANCIAL BID FORM

1. Financial Bid:

1.1 In accordance with the RFP Part 3 - Bid Preparation Instructions, 3.3 Section II - Financial Bid, the Bidder's Financial Bid must include this completed Form 3 to Part 4 – Bid Solicitation – Financial Bid Form.

1.2 Blank Prices in TABLE 2: Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price in TABLE 2 blank, a price will be assigned for evaluation purposes only based on the following:
i. The Average will be calculated based on all responsive Bidder's proposed prices for the same item the Bidder left blank.
ii. A price for evaluation purposes will be calculated using an 'Average plus 20%" calculation as follows: The Average is first calculated by entering all the responsive Bidders' price for the same item the Bidder left blank. The Average price is then increased by 20% to obtain the "Average plus 20%" price which will be used for evaluation of the Bidder's Financial Bid.
iii. If the Bidder becomes the recommended Bidder, prior to Contract award, the Contract price for the affected item(s) will be negotiated with the Bidder at a price not to exceed the Average price as calculated above. The negotiated price(s) will be incorporated into the Contract Price Schedule. Canada may request price support.

1.3 Estimated level of effort in TABLE 2 columns B and E are for evaluation purposes only and will not be included in the Contract Price Schedule.

1.4 ANNEX B - Price Schedule will be developed based on inputs in this Form from the winning Bidder.

2. Firm Lot Price

2.1 For the completion of the Work described in ANNEX A – SOW, Sections 1 through 8, the Bidder must propose a Firm Lot Price and Milestone Schedule in accordance with TABLE 1 below. The Total Firm Lot Price must not be less than $6,000,000.00 and must not exceed $11,000,000.00. The prices must be in Canadian currency, Customs Duties are included and Applicable Taxes are extra.

2.2 When completing the Milestone Schedule, Bidders must consider the following elements:

2.2.1 The Total Firm Lot Price must be broken down into milestone payments and the Bidder must indicate a proposed schedule for the milestone payments with payment frequency no more frequently than once a month. Milestones must be spaced as evenly as possible over the Contract and it should be clear what triggers the payment. The Bidder may propose fewer than 29 milestones, but must not propose more than 29 milestones.

2.2.2 Milestone payments must be subject to the completion and delivery of the milestone Work and its acceptance by the Technical Authority or his/her authorized representative. Milestones must be coordinated with the provision of a deliverable.

2.2.3 The Bidder must include a description of each proposed milestone, the amount of the milestone payment, and the proposed milestone due date expressed as the number of weeks or months after Contract Award. The description should provide sufficient detail to enable the Technical Authority to accurately determine whether the milestone has been met. The Bidder must provide a breakdown of the level of effort and other related costs necessary to achieve delivery of each associated milestone. The Bidder should review APPENDIX 2 to ANNEX A – Key Activities and ensure that the proposed Milestone Schedule for payment is in alignment with the Completion Dates for all Key Activities.

TABLE 1 - Firm Lot Price and Milestone Schedule	Sections 1 through 8 of ANNEX A - Statement of Work *(for financial evaluation)*		
(A) Milestone Description	**(B) Amount ($ CAD)**	**(C) Milestone Deliverables**	**(D) Delivery Due Date**
1	$0.00		
2	$0.00		
3	$0.00		
…	$0.00		
29	$0.00		
(E) Total Firm Lot Price [Sum of (B) for all Milestones, 1 through n]	**$0.00**		

3. As-and-when-requested work:

The Bidder must propose firm per diem rates in Table 2, for as-and-when-requested Work, to be performed pursuant to the Contract and any resulting Task Authorizations. The firm per diem rates must include the cost of labour, fringe benefits, general and administrative expenses, work estimates, travel, overhead, profit and the like, excepting only Applicable Taxes. The Contractor will not be permitted to charge per diem rates to prepare work estimates or Task Authorizations. The rates must be in Canadian currency, Customs Duties are included and Applicable Taxes are extra.

TABLE 2	AS-AND-WHEN-REQUESTED WORK (Section 9 of ANNEX A - SOW) – TASK AUTHORIZATIONS – Resource Categories *(for financial evaluation)*						
Resource Categories	**(A)** Initial Contract Period Firm All-Inclusive Per Diem	**(B)** Estimated Level of Effort (LOE) for (A) (Working Days)	**(C) Sub-total (AxB)**	**(D)** Option Periods Firm all-inclusive Per Diem	**(E)** Estimated LOE for (D) (Working Days)	**(F) Sub-total (DxE)**	**(G) Total Estimated Cost per Resource Category [C+F]**
Communications Consultant (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Courseware Developer (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Data Conversion Specialist (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Database Administrator (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Database Modeller (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00

Information Management Architect (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Programmer / Analyst – Business Objects (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Programmer / Analyst - MS Dynamics CRM (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
Web Developer (Level 3)	$0.00	120	$0.00	$0.00	120	$0.00	$0.00
						(H) Total Cost [Sum of (G) for all Resource Categories]	**$0.00**

4. Total Evaluated Bid Price:

The Total Evaluated Bid Price will be calculated as follows: Total Firm Lot Price (Table 1, E) + Total Estimated Cost for Resource Categories (Table 2, H) = Total Evaluated Bid Price

Actual Total Evaluated Bid Price:	**$0.00**