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

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

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
KIA 0S5

Title - Sujet ISS Transformation - RFP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 002
Client Reference No. - N° de référence du client 20170549	**Date** 2017-05-18
GETS Reference No. - N° de référence de SEAG PW-$$XE-678-31237	
File No. - N° de dossier 678xe.EP243-170549	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-07-14**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Oates, Christine	**Buyer Id - Id de l'acheteur** 678xe
Telephone No. - N° de téléphone (873) 469-3917 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

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

Amendment Number 002

Purpose:

The purpose of this amendment is to extend the closing date of this Request for Proposal (RFP), publish the presentation from the Bidders' Conference, to identify changes to the RFP and to provide answers to questions received with regards to this RFP.

A. CHANGES

Amendment number 002 is raised to identify the following changes to the RFP:

Change 4:

At ANNEX A, Section 1, 1.1.2.1 Project Objectives:

DELETE:

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.

INSERT:

Included within the scope of the ISST project is business process re-engineering where appropriate to align the ISS business and the proposed unified solution.

Change 5:

At ANNEX A, Section 1, under 2.1 New Solution:

DELETE:

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.

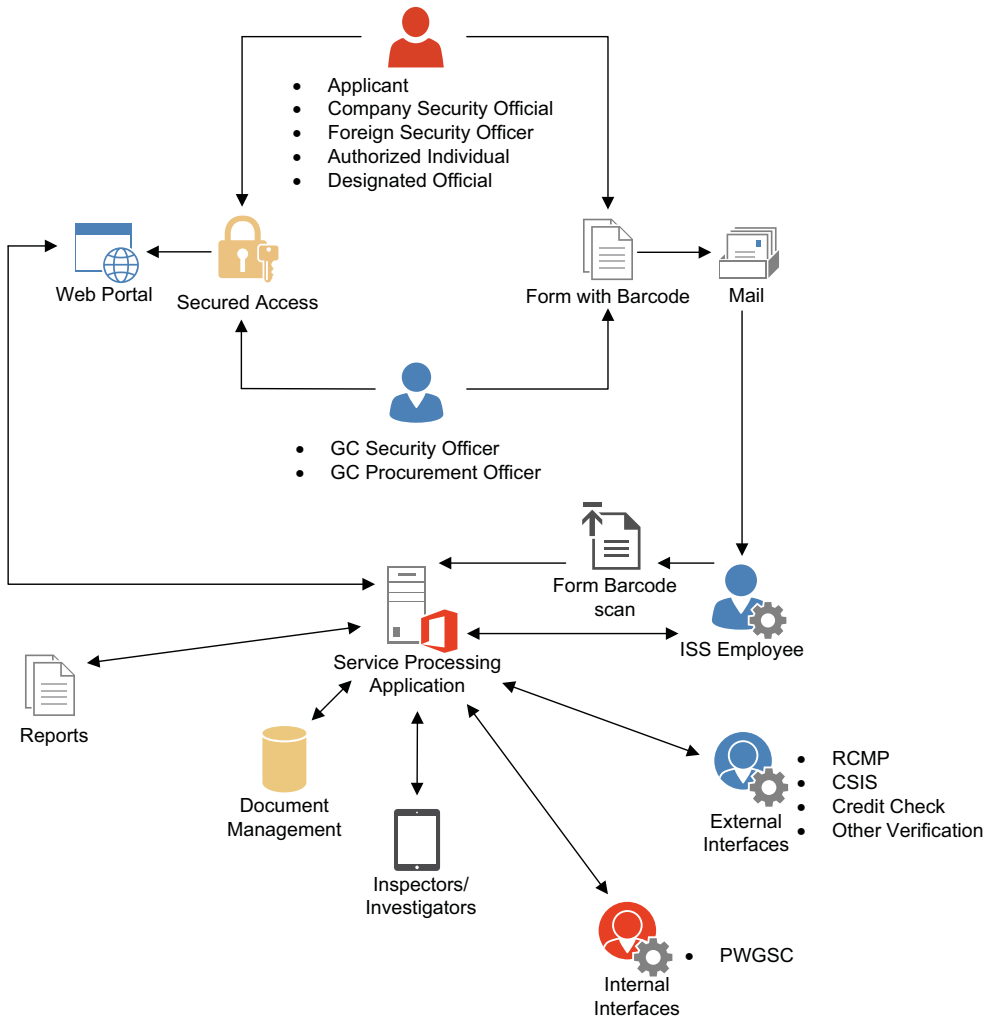
The ISST Solution's Service Processing Application will be used to process the submitted service requests with external to and internal government interfaces. For example, the ISST Solution will interact with the Royal Canadian Mounted Police (RCMP) to perform criminal record checks for personnel security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

INSERT:

The following diagram illustrates the high level interaction map for the required ISST Solution. Illustrated are the high level user types utilizing GC Secured Access 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 forms information into the ISST Solution's Service Processing Application.

The ISST Solution's Service Processing Application will be used to process submitted ISS service requests. The ISST Solution's Service Processing Application will support processing of these service requests through external and internal interfaces with ISS security partners. 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 for CSP and CGP inspectors and investigators.

REPLACE Figure 1: ISST Solution high level interaction map, with the following:



Change 6:

At ANNEX A, Section 2: Business Requirements, under 1.2 Detailed Requirements – Business Process Re-engineering:

DELETE:

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.

INSERT:

BR.07	Perform a Gap Analysis after business process re-engineering and Solution design to identify areas (e.g. business processes and users) for Change Management engagement.

Change 7:

At ANNEX A, Section 2: Business Requirements, under 2.2.1 Service Processing Application:

DELETE:

APP-AU.02	The automatic issuing of appropriate approval certificates (e.g. personnel screening briefing certificate): (a) For service request satisfying all identified 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-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.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.
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 be compatible with automated data rationalization.
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.27	Enables Internal Users to retrieve archived records from a case file for a specified period of time.
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).

INSERT:

APP-AU.02	The automatic issuing of appropriate approval certificates (e.g. personnel screening briefing certificate): (a) For service request satisfying all 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-OPS.21	Enables Internal Users with appropriate permissions to, on demand, update a sandbox environment with a copy of the solution from production (application only, no data) for the purpose of refreshing the sandbox environment.
APP-OPS.24	Enables the ability to disable 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.
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.
APP-IM.13	Enables data and information acquisition throughout a case lifecycle (e.g. an organization's security request for ISS' Document Safeguarding Capability will require acknowledgment of compliance before the security clearance can be granted).
APP-IM.27	Enables Internal Users to retrieve archived records from a case file for a specified retention time, determined by the business process.
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 images or record video, and append the files to the case.).

Change 8:

At ANNEX A, Section 2: Business Requirements, under 2.2.1 Service Processing Application:

DELETE:

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.

Change 9:

At ANNEX A, Section 2: Business Requirements, under 2.2.2 Web Portal

DELETE:

WP-SH.02	Uses approved government methods for user identification and authentication (e.g. GC Pass, GCKey, MyKey, etc.).
WP-CH.02	Enables External Users to send/receive messages to/from ISS.
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.
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.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-RP.04	Enables External Users to save or print the reports on demand.

INSERT:

WP-SH.02	Uses approved government methods for user identification and authentication (e.g. Secured Access, GCKey, MyKey, etc.).
WP-CH.02	Enables External Users to send/receive email messages to/from ISS.
WP-UE.03	Enables authorized External Users (e.g. Security Official) to complete service requests on behalf of other External Users. 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.
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 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 functionality.
WP-UE.06	Enables External Users to access the web portal from tablets equipped with major Internet browsers, without any loss of portal functionalities.
WP-UE.10	External Users can print completed forms containing all inputted information for their records or for submission to the ISS for processing.
WP-UE.11	Provides access to downloadable fillable forms that must contain same data as their online counterparts.
WP-RP.04	Enables External Users to save-as or print the reports on demand.

Change 10:

At ANNEX A, Section 2: Business Requirements, under 2.2.2 Web Portal

DELETE:

WP-UE.07	Enables External Users to access an abridged version of the web portal from smartphones.

Change 11:

At ANNEX A, Section 3: Technical Requirements, under 1.1 Requirements Overview:

DELETE:

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 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.

INSERT:

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 Secured Access 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.

Change 12:

At ANNEX A, Section 4: Secure Access, under 1.1 Requirements Overview:

DELETE:

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.

INSERT:

For the Internal User group, the secure access provided by the Contractor must interoperate with GC's Identity, Credential and Access Solution (Secured Access (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 Secured Access to better serve the GC security needs.

Change 13:

At ANNEX A, Section 5: IT Security Requirements, 1.1 Requirement Overview, under 1.1.1 Security Assessment and Authorization Process:

Following the first paragraph, **INSERT:**

The SA&A process follows the Systems Development Life Cycle with three gates identified. The Gate 1 assessment is performed during the design phase. Gate 2 is performed during the development phase and Gate 3 is prior to deployment. As well, all subsequent system changes following deployment are subject to a Security assessment. Canada will review and analyze the evidence provided of how the requirements/controls are met using the documents described below. A Security Assessment Report will be written by GC and any corrective action required for the Solution must be performed as requested by GC.

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.

Change 14:

At ANNEX A, Section 5: IT Security Requirements, under 1.2 Detailed Requirements:

DELETE:

SC.30	The Solution must establish and manage cryptographic keys in accordance with guidelines promulgated by CSE.

INSERT:

SC.30	The Contractor must ensure that the solution is configured to establish and manage cryptographic keys securely (according to CSE) when establishing communication or encrypting data at rest.

Change 15:

At ANNEX A, Section 6: Testing Management, under 1.2 Detailed Requirements

DELETE:

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.

INSERT:

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 all defects found before performing the next-stage testing; and

	(d) Ensure testing cycles continue until a full cycle is completed with minimal bugs or acceptable defects, as approved by the Project Authority. 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 with minimal bugs or acceptable defects, as approved by the Project Authority; (e) The Contractor must log and address all testing defects before final-sign off can be obtained from the Project Authority.

Change 16:

At ANNEX A, Section 7: Management and Oversight, under 1.1 Project Governance:

DELETE:
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.

INSERT:

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 (in consideration of all requirements including security requirements);
(e) Solution Development and Implementation services In accordance with all business technical and security requirements; and
(f) Data migration services as defined in section 2.2.3.

Change 17:

At ANNEX A, Section 8: Solution Sustainment, under 1.1 Requirement Overview:

DELETE:

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.

INSERT:

The Contractor is responsible for the design and development of materials, processes and activities that will be used by the ISS and PWGSC CIOB and SSC for the ongoing support and maintenance of the Solution once the Solution has been released.

Change 18:

At ANNEX A, Section 8: Solution Sustainment, under 1.2 Detailed Requirements:

INSERT:

SS.10	Subject to Project Authority approval, the Contractor may be requested to exercise additional/optional services related to Solution sustainment on an as and when requested basis through the issue of a Task Authorization.

Change 19:

At APPENDIX 3 to ANNEX A – User Accounts:

DELETE:

Section 2. Internal Users in its entirety.

INSERT:

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 Clerk

The Clerk role is a limited processing or modification role. The main function of the clerk role is to perform service request triage and to assist in the routing of case files for processing.

Function	Actions Permitted
General	1) Search cases and case information; 2) View case and case information.
Processing	1) Limited service request processing; 2) Trigger security partner checks; 3) Limited service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request); 4) Input service request processing data (e.g. justifications or rationale's on taken decisions or scanning of barcodes to input a service request submission); 5) Assign case files for further processing; 6) Input case notes;

	7) Attach files of various formats to the case file; 8) Close case files.
Notifications/ Correspondence	1) Generate and send notifications; 2) Generate and send correspondence; 3) Attach notifications and correspondence to case file; 4) Set internal reminder notifications for follow-up activities;
Reporting	1) Generate available predetermined reports.

2.2 Analyst

The Analyst role performs the processing of service requests. The Analyst role includes such business functional roles as registration analyst, compliance inspectors, investigators, call center analysts, quality control, etc.

Function	Actions Permitted
General	1) Search cases and case information; 2) View case and case information.
Processing	1) Full service request processing; 2) Trigger security partner checks; 3) Trigger internal sub processes (e.g. trigger a compliance inspection request); 4) Limited service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request); 5) Input service request processing data (e.g. justifications or rationale's on taken decisions or inspection/investigation reports or scanning of barcodes to input a service request submission); 6) Open case files that may or may not be linked to existing cases; 7) Assign case files for further processing; 8) Input case notes; 9) Create and manage scheduled activities (e.g. inspectors create blocks of inspections within geographical areas to maximize travel costs); 10) Attach files of various formats to the case file; 11) Close case files.
Notifications/ Correspondence	1) Generate, edit and send notifications; 2) Generate, edit and send correspondence; 3) Attach notifications and correspondence to case file; 4) Set internal reminder notifications for follow-up activities.
Reporting	1) Generate available predetermined reports.
Approvals	1) Provide necessary approvals (e.g. CGP Compliance Travel Coordinator approves submitted travel requests before travel arrangements are made).

2.3 Senior Analyst

The Senior Analyst role performs the same actions as the analyst with more privileges to perform maintenance activities. Senior Analysts are generally team leads or section chiefs.

Function	Actions Permitted
General	1) Search cases and case information; 2) View case and case information.
Processing	1) Full service request processing; 2) Trigger security partner checks; 3) Trigger internal sub processes (e.g. trigger a compliance inspection request);

	4) Service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request); 5) Edit service request processing information, no modification to data submitted with the service request; 6) Input service request processing data (e.g. justifications or rationale's on taken decisions or inspection/investigation reports or scanning of barcodes to input a service request submission); 7) Open case files that may or may not be linked to existing cases. 8) Assign case files for further processing; 9) Input case notes; 10) Edit existing case notes; 11) Create and manage scheduled activities (e.g. inspectors create blocks of inspections within geographical areas to maximize travel costs); 12) Attach files of various formats to the case file; 13) Manage supporting documents and files attached to case files; 14) Close case files.
Notifications/ Correspondence	1) Generate, edit and send notifications; 2) Modify notification templates; 3) Generate, edit and send correspondence; 4) Modify correspondence templates; 5) Attach notifications and correspondence to case file; 6) Set internal reminder notifications for follow-up activities for themselves and other analysts.
Reporting	1) Generate available predetermined reports.
Maintenance	1) Delete
Approvals	1) Provide necessary approvals (e.g. the CGP Senior Analyst will set the status of registered sites to active for CGP registration's prior to approving the organizations registration request); 2) Provide necessary approvals and sign-off as required to finalize service request processing (e.g. CSP Senior Analyst approves and signs off on the granting letter when an organizations registration request is approved).

2.4 Manager/Director

The Manager role is mostly read only for informational purposes with the ability to provide approvals were required.

Function	Actions Permitted
General	1) Search cases and case information; 2) View case and case information.
Processing	1) Assign case files for further processing; 2) Input case notes; 3) Edit existing case notes; 4) Attach files of various formats to the case file; 5) Manage supporting documents and files attached to case files; 6) Service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request); 7) Input service request processing data (e.g. justifications or rationale's on taken decisions or inspection/investigation reports or scanning of barcodes to input a service request submission).
Notifications/ Correspondence	1) Generate, edit and send correspondence;

Reporting	1) Generate available predetermined reports.
Approvals	1) Provide necessary approvals (e.g. the CSP Director approves suspension); 2) Provide necessary approvals and sign-off as required to finalize service request processing (e.g. Compliance Manager will review inspection reports for sign-off on them as part of the process to approve an organizations registration request).

2.5 Read Only User

Read only user roll that can search and view data but cannot make any modifications or generate any notifications, correspondences or reports.

Function	Actions Permitted
General	1) Search cases and case information; 2) View case and case information.

2.6 System Administrator

The Systems Administrator role is a read only role for the sole purpose of performing system level business maintenance that requires controlled access. The activities performed by the System Administrator requires intimate knowledge of the Solution and business functions to perform these actions.

Function	Actions Permitted
General	1) Search cases and case information; 2) View case and case information.
Maintenance	1) Create and edit notification templates; 2) Create and edit correspondence templates; 3) Create, disable, delete and modify user accounts (e.g. user account tombstone information); 4) Add or remove available capabilities or roles to user accounts; 5) Add, modify, delete or disable capabilities that are available to be assigned to a user role; 6) Add, modify, delete or disable existing business rules/processes utilized by the solution as a whole (e.g. both the external facing web portal and internal processing application) for the implementation of future policies and business rules/processes; 7) Add, modify, delete or disable, workflows within the solution; 8) Maintain business forms for case processing (i.e. add new data fields to forms to capture additional information or to disable existing data fields if no longer required); 9) Modify externally facing forms and publish them to the solutions web portal; 10) Add, modify, delete or disable whole or parts of the solution; 11) Maintain access control and permissions at the field level at the user role level; 12) Update a sandbox environment with a copy of the solution from production (application only, no data); 13) Ability to enable/disable a link displayed on the solutions web portal (Business Requirement APP-OPS.22); 14) Maintain access to the various environments used to support the solution.
Reporting Maintenance	1) Generate available predetermined reports. 2) Add, modify, delete or disable reports available within the solution;

	3) Add, modify, delete or disable selection criteria associated to a report; 4) Add, modify, delete or disable reports that can be accessed by user roles and/or user accounts; 5) Add, modify, delete or disable custom report queries, which may or may not result in a new solution available report.
Approvals	1) Approval of user account requests.

Change 20:

DELETE APPENDIX 4 to ANNEX A – Legislative, Regulatory and Policy Requirements in its entirety, and **REPLACE** with the attached APPENDIX 4 to ANNEX A – Legislative, Regulatory and Policy Requirements.

B. QUESTIONS

Question 4:

Bidders have submitted many questions, but few answers have been provided to date. Also, at the Bidders' Conference, Canada indicated that some items of the RFP were under review. In order to provide time for Canada to answer the outstanding questions, provide any changes resulting from further review of the RFP requirements, and for Bidders to adjust their responses, we respectfully request an extension to June 30, 2017.

Answer 4:

Canada remains committed to providing responses to Bidders' questions, and acknowledges that many questions received with respect to this RFP are outstanding. Canada has reviewed certain requirements of the RFP in response to questions, and has identified areas where changes are required. These changes are forthcoming, and Canada intends to publish these identified changes on or before May 29, 2017.

In consideration of outstanding responses to Bidder questions, and of the forthcoming changes to the RFP, Canada extends the closing date of the RFP to 2:00 PM (EDT) on July 14th, 2017.

Question 5:

Due to the overall complexity of the requirements, as well as the resultant impact of the changes and clarifications provided at the Bidder's conference, we request an extension to June 23.

Answer 5:

See the response provided to Question 4 in this Amendment.

Question 6:

Given the recent clarifications on the reference requirements provided at Industry Day, is PSPC able to extend the bid close date to June 23? This would allow organizations more time to ensure compliance on the references.

Answer 6:

See the response provided to Question 4 in this Amendment.

Question 7:

We are hereby requesting an extension to the bid close date. Our request is to extend the bid close date to June 30, 2017.

Answer 7:

See the response provided to Question 4 in this Amendment.

Question 8:

Given the scope and complexity of the RFP requirements, as well as with the outstanding questions that are being reviewed, it is requested that the closing date of the solicitation be extended to no earlier than June 30, 2017.

Answer 8:

See the response provided to Question 4 in this Amendment.

Question 9:

Could you please either send or post the PowerPoint presentation from the May 5th Bidders' Conference?

Answer 9:

A copy of the Bidders' Conference presentation is attached to this Amendment.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

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. The Project Authority will advise the Contractor of any new or amended federal legislation, regulations, policies, directives, standards and guidelines that impact the project.

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	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32495
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
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/27578
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/1842/html/26717
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
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/node/270/html/10572
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 Authorization form (TBS/SCT 330-23E)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-eng.asp
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
Security incident report for company security officers and alternate company security officers	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/rapport-incident-report-eng.html
Reporting security incidents	http://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/signalement-reporting-eng.html
Company security officer or alternate company security officer attestation form	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/attestation-eng.html
Consent to release of reliability screening and/or security clearance information	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/cnsntmnt-cnsnt-eng.html
Company security officer's guide to completing and submitting personnel security screening forms	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/index-eng.html
How to complete the personnel screening, consent and authorization form (TBS/SCT 330-23E)	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/330-23-eng.html
How to complete the security clearance form (TBS/SCT 330-60E)	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/330-60-eng.html
How to complete the security screening certificate and briefing form (TBS/SCT 330-47)	http://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/guide/330-47-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://www.tpsgc-pwgsc.gc.ca/esc-src/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
Obtain security screening for your organization	http://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/enquete-screening-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-4 to annex 5-D – Post-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a4-eng.html
Annex 5-C - Standard for the Transmittal of CLASSIFIED and PROTECTED Information and Assets	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5c-eng.html
How to transfer sensitive information and assets	http://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/transfert-transfer-eng.html
Visits	
Request for visit form	http://www.tpsgc-pwgsc.gc.ca/esc-src/formulaires-forms/visite-visits-eng.html
Approval for visits to secure sites	http://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/visite-visit-eng.html

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

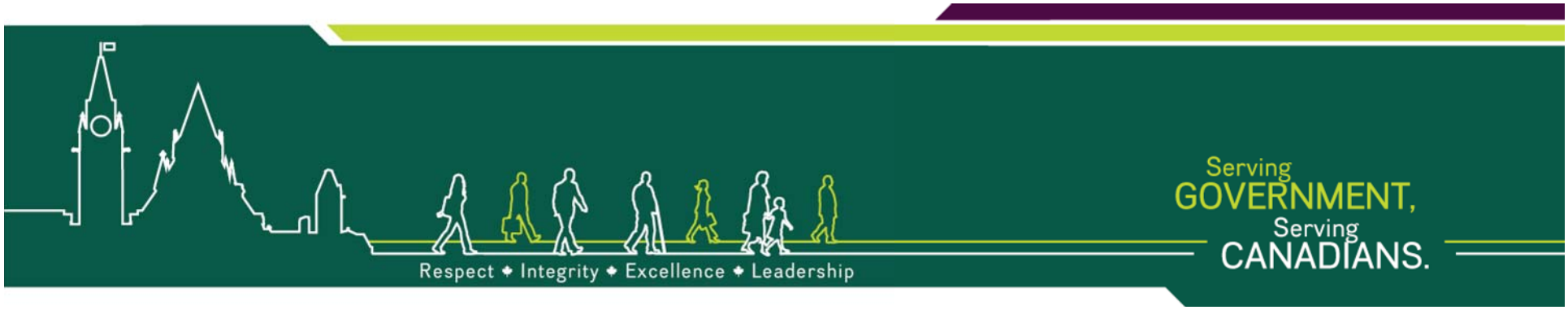
7. CONTROLLED GOODS PROGRAM - FORMS AND GUIDELINES

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 checklist	http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/comment-how/liste-checklist-eng.html
Developing a security plan for controlled goods	http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/comment-how/ps-sp-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).



Industrial Security Systems Transformation Bidders' Conference

EP243-170549/B

Public Services and Procurement Canada (PSPC)

May 05, 2017

Agenda

- Procurement Overview
- Statement of Work Overview
  - Business Requirements
  - Technical Requirements
  - Project Governance and Management
  - Change Management and Sustainment
- Evaluation Criteria: Mandatory and Rated
- Questions

Note: Information provided orally by Canada is not binding on Canada unless put in writing as a formal amendment to the RFP. Bidders are to follow the written RFP instructions and requirements in preparing bids.

Objectives

1. To provide a brief overview of the Industrial Security Systems Transformation (ISST) Request for Proposal.

2. To provide industry an opportunity to bring forth questions and provide a forum for discussion.

Procurement Strategy

- Continued engagement and consultation with industry throughout the solicitation process.

- Engagement with key internal stakeholders (e.g. PSPC: Chief Information Officer Branch (CIOB), Clients (other Departments/Agencies; Clients (Industry users).

Procurement Process

- **Draft RFP:**
  - ✓ Standard “Q & A” period solicited early supplier feedback and addressed supplier questions.
- **Final RFP:**
  - ✓ Incorporated supplier responses to Draft RFP where possible.
  - ✓ Standard “Q & A” period to further address any outstanding questions or concerns from suppliers.
  - ✓ Bidders’ Conference to highlight overall requirements and evaluation methodology, and provide forum to raise supplier questions.

Procurement Process

- **Evaluation and Selection Methodology**
  - 70 % Technical + 30 % Financial
  - Technical Bid Evaluation
  - Financial Bid Evaluation

- **Basis of Payment**
  - Fixed Firm Lot Price (Milestone payments)
  - Optional Services

Procurement Process

- **Enquiries:**
  - All enquiries must be submitted in writing via e-mail to the Contracting Authority.
  - Bidders are requested to submit enquiries at least 10 calendar days before the bid closing date. Enquiries received after that time may not be answered.
- **Bid Submission:**
  - Must be received by Bid Receiving Unit
  - No conditional bids
  - Only one bid
  - 3 Sections : Technical Bid, Financial Bid, Certifications

ISST Background

- ISS services are public facing, directly serving Canadians and Canadian Industry
- Need to improve service delivery while contending with increased demand
- IT systems have reached the end of their sustainable lifecycle

Key Objectives

Increased Capacity:	Stable, reliable and responsive system performance and availability, regardless of the number of users.
Better Service:	One stop shop that is easier and faster to use, with fewer steps and hurdles and includes built-in support.
Better Information:	Allows users to track current clearance requests and run reports on past and current organization clearance activities.
Greater Efficiencies:	Less time spent filling out forms, correcting information, handling paper and waiting for assistance.
Greater Satisfaction:	User-friendly environment that supports faster clearance processing and provides self-service functionality

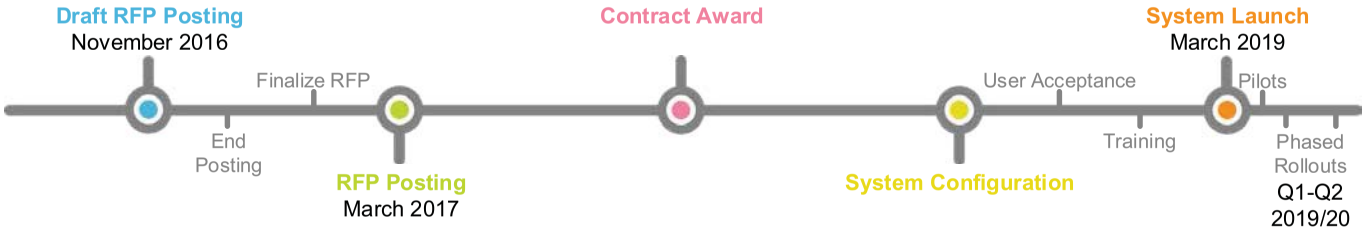
Minimize Paper ***Minimize Manual Process*** ***Minimize Process Steps*** ***Maximize Efficiencies***

Approach and Milestones

Approach:

- Comprehensive Business Process Analysis and Re-engineering
- Continuous Stakeholder Engagement
- Robust Change Management

Draft RFP Posting	November 2016
RFP Posting	March 2017
System Launch	March 2019



Annex A – Statement of Work

Business Requirements

The business requirements outline GC's expectations for business process re-engineering and the service application and web portal deliverables. The expected outcomes include:

Business Process Re-Engineering	Service App and Web Portal
Less steps in processes overall	More flexibility to manage business change and set standards
Increased automation to minimize potential for errors	Improved user experience to provide self-help and validation functionality
New processes and process mapping to support system and sustain standard approaches	Unified system for improved reporting capacity and data linking
Reduction in dependency of paper based activities	Efficient system to improve reliability and processing times

Annex A – Statement of Work

Technical Requirements

The ISST Solution should leverage the technology footprint identified in the ISST solution architecture and must be user friendly, reliable, maintainable, scalable, interoperable, and compliant with GC IT/IM policies, guidelines and environment.

Highlights and Solution Architecture
Develop Logical and Physical architecture blueprints
Conformance with WCAG and GC Web Standards guidelines and requirements
Secure access for External Users via Web Portal using GCKey and Secure-Key Concierge services
Secure access for Internal Users
Off-line access capabilities provided by MS Dynamics CRM for Outlook
Information sharing with partner organizations automated and managed using GCIP capabilities
Managed Secured File Transfer (MSFT) available service for file exchange

Annex A – Statement of Work

Security Requirements

- This procurement is subject to National Security Exception and is limited to Canadian Companies and Canadians (including permanent residents);
- Subcontracting must be approved by the Project Authority;
- Access to ISS sensitive information and IT systems requires security clearance at Secret level (at minimum). All other accesses requires Reliability status (at minimum);
- IT Security must be embedded into the fabric of the Solution.

Annex A – Statement of Work

Governance

Governance of the solution will ensure that roles are defined, decisions are made quickly and authoritatively and that information is properly disseminated. Participating shops include two branches within Public Works and Government Services Canada, one branch with Shared Services Canada and the Contractor.

PWGSC ISS	PWGSC CIOB	SSC	Contractor
Decisions having project/business impacts	Represent CIOB interests	Designing and implementing support infrastructure	Solution design, development and delivery
Review and approve project deliverables	Review and approve technical (IT) deliverables	Ensuring infrastructure security	Process Re-engineering, Data migration and Change management
Support contractor with project activities	Ensuring engagement with IT stakeholders	Participating in infrastructure performance testing	Project management and planning

Annex A – Statement of Work

Management and Oversight

The project management requirements are intended to ensure that the Solution delivered at the end of the project meets the expected outcomes.
Project scope is defined and controlled
Project schedule is monitored and respects committed timelines
There is awareness of project risks and recommendations on approaches for their mitigation
There are no compromises to the project's quality and the solution meets its intended objectives

Change Management & Sustainment

The change management and solution sustainment requirements are intended to ensure that the "as-is" state successfully transitions to the "to-be" state, with minimal interrupts and maximum adoption, and that the "to-be" state is effectively sustained.
Stakeholder identification and change readiness assessments
Identifying tools for communication and collecting feedback
Role specific training and support documentation
Developing new system support processes and recommendations

Project deliverables are to be supported by effective planning, reporting and evaluation activities.

Contractor will assist ISS in transitioning to the Center of Expertise (COE) to provide system administration and support.

Technical Evaluation: Mandatory Criteria

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. Bids which fail to meet the mandatory criteria will be declared non-responsive and will not be considered further.

Criteria	Description

M1 and M2	• For each of M1 and M2:
	  • Bidder must provide **3** Reference Projects
	  • **2** projects must have been completed within **15** years of the date of Bid Closing
	  • **1** project must have been completed within **5** years of the date of Bid Closing
	  • **All 3** projects must have had a public-facing internet-based information exchange component

M1	• **All 3** projects must have provided Business Process Re-engineering **and** Change Management services • **1** project must have provided **all** of the Business Process Re-engineering services described • **1** project must have provided **all** of the Change Management services described
M2	• **2** projects must have provided **3** of the following **6** activities; IT design, configuration, development, implementation, integration and data migration services • **1** project must have provided **all** of the following **4** activities; IT design, implementation, integration and data migration services and **1** of the following **2** activities; configuration or development
M3	• The Bidder must provide an accessible Customer Reference with accurate contact information to validate **each** Reference Project

Technical Evaluation: Point Rated Criteria

- Bids which meet all the mandatory criteria will be evaluated against the Point Rated Criteria, and scored as specified in Attachment 1 to Part 4. It is mandatory that proposals meet the overall minimum pass mark of 70%, which is 1750 points.

- Bids meeting the overall minimum pass mark will be deemed responsive.

- The relative weight of each rated requirement is determined by points allocated to its respective section.

Technical Evaluation: Point Rated Criteria

Criteria	Description
R1	Project Management (Maximum 620 Points) ▪ Preliminary Project Management Plan ▪ Project Governance; Scope Management; Schedule Management Plan; Project Schedule; Risk Management; Quality Management.
R2	Business Process Re-engineering (Maximum 360 Points) ▪ Business Process Re-engineering strategy ▪ Understanding of current business processes and operations; Plan for gap analysis; Understanding of constraints and impacts; Proposed process improvements and implementation approach; Understanding of risks and risk mitigation options; Scheduling of BPR Activities.
R3	Relationship Management (Maximum 170 Points) ▪ Relationship Management Approach ▪ Overall GC and SI relationship management approach; Communications approach in respect of proposed governance structure; Issue management and resolution; Planning and management of changes.
R4	Security Management (Maximum 360 Points) ▪ Concept of Security Operations

Technical Evaluation: Point Rated Criteria

Criteria	Description
R5	Sensitive Data Migration (Maximum 200 Points) ▪ Approach to Data Migration ▪ Key activities; Defined roles and responsibilities; Risks and mitigation strategies; Security considerations.
R6	Change Management Plan (Maximum 380 Points) ▪ Preliminary Change Management Plan ▪ Understanding of requirements; Key considerations; Evaluation method to assess effectiveness.
R7	Testing Plan (Maximum 170 Points) ▪ Preliminary Testing Plan ▪ Consideration of SC-42 and Section 6 requirements; Adequate coverage to ensure readiness; Identification and management of risks.
R8 & R9	Corporate Reference Projects (Maximum 80 and Maximum 160 Points, Respectively) ▪ Up to 3 reference projects (R8) that have successfully delivered a Government of Canada solution ▪ Up to 3 reference projects (R9) that have successfully delivered a solution using a Case Management and/or Microsoft Dynamics CRM, which required IT design and configuration

Questions

20