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**<br>ISS Transformation - RFP | |
| **Solicitation No. - N° de l'invitation**<br>EP243-170549/B | **Amendment No. - N° modif.**<br>011 |
| **Client Reference No. - N° de référence du client**<br>20170549 | **Date**<br>2017-09-13 |
| **GETS Reference No. - N° de référence de SEAG**<br>PW-$$XE-678-31237 | |
| **File No. - N° de dossier**<br>678xe.EP243-170549 | **CCC No./N° CCC - FMS No./N° VME** |
| **Solicitation Closes - L'invitation prend fin**<br>**at - à** 02:00 PM<br>**on - le** 2017-10-02 | **Time Zone**<br>**Fuseau horaire**<br>Eastern Daylight Saving Time EDT |
| **F.O.B. - F.A.B.**<br>**Plant-Usine:** □ **Destination:** ☑ **Other-Autre:** □ | |
| **Address Enquiries to: - Adresser toutes questions à:**<br>Oates, Christine | **Buyer Id - Id de l'acheteur**<br>678xe |
| **Telephone No. - N° de téléphone**<br>(873) 469-3917 ( ) | **FAX No. - N° de FAX**<br>( ) - |
| **Destination - of Goods, Services, and Construction:**<br>**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**

## Amendment Number 011

**Purpose:**

A. To identify changes to the (Request for Proposal) RFP.
B. To provide answers to questions received with regards to this RFP.
C. To extend the closing date of this RFP to October 2, 2017.

---

## A. CHANGES

### Change 91:

At ANNEX A, SECTION 1: CANADA'S INDUSTRIAL SECURITY SOLUTION OVERVIEW, under 2.1 New Solution, **DELETE: Figure 1:** ISST Solution high level interaction map. in its entirety, and **REPLACE** with the following:

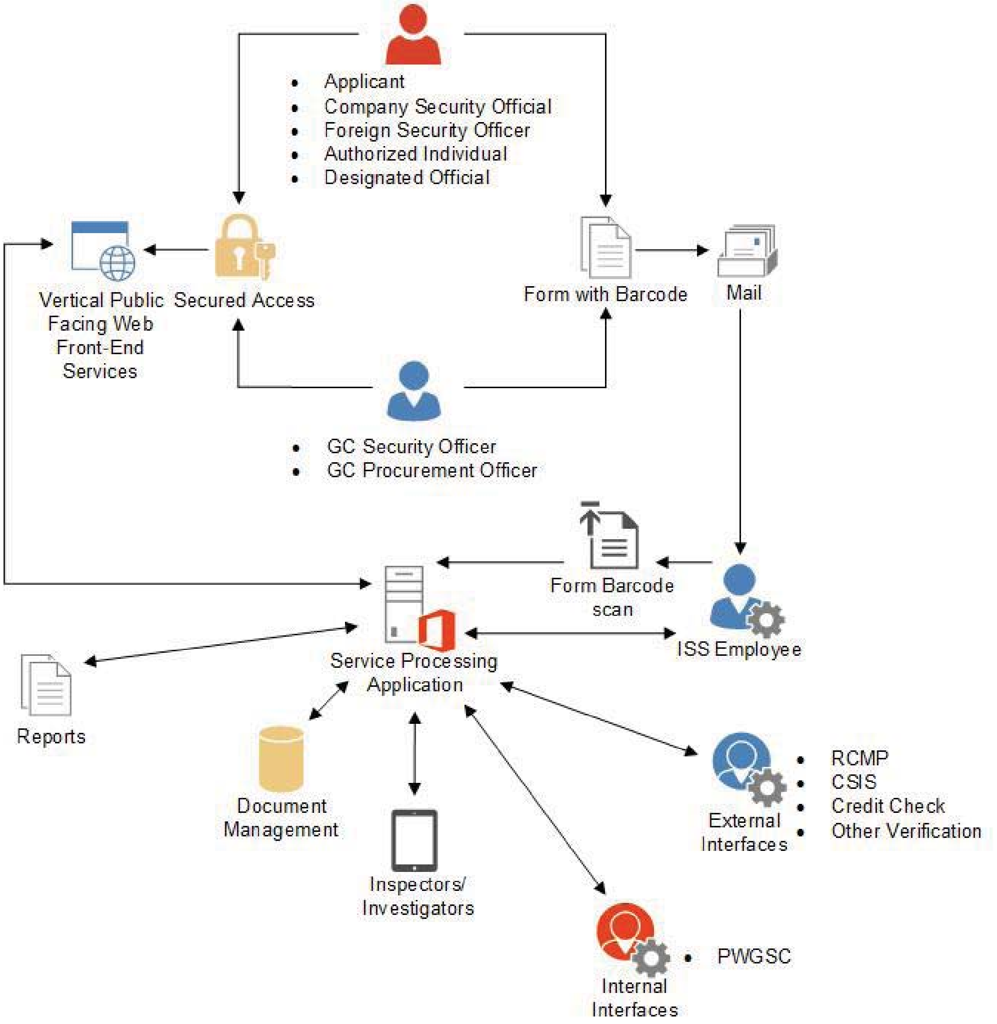


**Figure 1:** ISST Solution high level interaction map.

**DELETE:**

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.

**INSERT:**

Illustrated are the high level user types utilizing GC Cyber Authentication Services technology to access the ISST Solution’s Vertical Public Facing Web Front-End Service in order to submit service requests to the ISST Solution’s Service Processing Application. Please refer to http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262 for more information on the GC Cyber Authentication Service.

**Change 92:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 1.2 Detailed Requirements – Business Process Re-Engineering:

**INSERT:**

| | |
|---|---|
| BR.19 | Prepare a Preliminary Business Process Re-engineering Strategy which includes, but is not limited to:<br>(a) An understanding of the current ISS business processes and the need for security practices within the various business operations;<br>(b) A plan to conduct a business process gap analysis;<br>(c) An understanding of constraints and impacts;<br>(d) Four examples of opportunities to improve process efficiency and effectiveness and proposed implementation approaches;<br>(e) An understanding of risks and options for risk resolution or mitigation; and<br>(f) Scheduling of business process re-engineering activities. |
| BR.20 | Prepare a Business Process Re-engineering Strategy after the Preliminary Business Process Re-engineering Strategy has been evaluated by Canada and deemed that the strategy meets the benefits and requirements identified above. |

**Change 93:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.1 Requirement Overview – Functional Requirements:

**DELETE:**

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

**INSERT:**

The Solution is a business application composed of two major components: a Service Processing Application and a Vertical Public Facing Web Front-End Service.

**DELETE:**

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:

**INSERT:**

The Vertical Public Facing Web Front-End Service 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 Vertical Public Facing Web Front-End Service that:

**Change 94:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-AU.02, item d) in its entirety and **REPLACE** with the following:

d) Availability of appropriate approval certificate to the External User for download/printing from the Vertical Public Facing Web Front-End Service.

**Change 95:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-AU.04 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| APP-AU.04 | Automatic population of the External User's Vertical Public Facing Web Front-end Services calendar feature with pre-defined events relating to service requests submitted to ISS (e.g. correspondence due dates, organizational registration renewals, etc.). |

**Change 96:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-OPS.07 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-end Service and internal processing application. For example, to be able to modify the solution parameter defining the standard number of days to complete a CGP registration request. This is then automatically reflected on all reports and dashboards and used in all internal calculations. |

**Change 97:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-OPS.10 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| APP-OPS.10 | Enables Internal Users with appropriate permissions to modify externally facing forms and publish them to the Vertical Public Facing web front-end service. |

**Change 98:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-OPS.19 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-end Service. This is to allow the Internal User to see what the External User is seeing on screen and vice versa. |

**Change 99:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-OPS.22 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| APP-OPS.22 | Enables Internal Users with appropriate permissions to enable and disable a link that External Users can access from the Solution Vertical Public Facing Web Front-End Service to gain access to the Sandbox/Training environment. See business requirement WP-UE.22. |

**Change 100:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-COM.06 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-end Services to CGD Authorized Individuals). |

**Change 101:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-PPL.03 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-end Service 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). |

**Change 102:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-ICN.04 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-end Service into the processing application. It must also be available as an option to be triggered by Internal Users on demand. |

**Change 103:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-RP.12 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Solution's suite of standard reports externally (Vertical Public Facing Web Front-end Service) and internally (processing application). |

**Change 104:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 – Service Processing Application, **DELETE** APP-RP.14 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| APP-RP.14 | Enable Internal Users to modify the selection criteria associated to the standardized reports that is available to External Users on the Vertical Public Facing Web Front-end Service. |

**Change 105:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, **DELETE** heading at 2.2.2 – Web Portal and **REPLACE** with heading 2.2.2 – Vertical Public Facing Web Front-End Service.

**Change 106:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 – Vertical Public Facing Web Front-End Service:

**DELETE:**

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

**INSERT:**

The Contractor must deliver a Vertical Public Facing Web Front-End Service that provides the following functionalities, but is not limited to:

**Change 107:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 – Vertical Public Facing Web Front-End Service, **DELETE** WP-SH.05 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| WP-SH.05 | Enables a synchronous exchange of information between the Vertical Public Facing Web Front-End Service and the Services Processing Application. |

**Change 108:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 – Vertical Public Facing Web Front-End Service, **DELETE** WP-UE.05 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| WP-UE.05 | Enables External Users to use common mobile devices that are equipped for Internet browsing to access the Vertical Public Facing Web Front-end Service at any time using any device. This includes electronic signatures. |

**Change 109:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 – Vertical Public Facing Web Front-End Service, **DELETE** WP-UE.06 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| WP-UE.06 | Enables External Users to access the Vertical Public Facing Web Front-end Service from tablets equipped with Internet browser, without any loss of Vertical Public Facing Web Front-end Service Functionalities. |

**Change 110:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 – Vertical Public Facing Web Front-End Service, **DELETE** WP-UE.17 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| WP-UE.17 | Enables External Users to navigate throughout the Vertical Public Facing Web Front-end Service in a manner that is consistent with the GC Web Standards. |

**Change 111:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 – Vertical Public Facing Web Front-End Service, **DELETE** WP-UE.22 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-end Service functionalities and not retain or transmit any data during the course of its usage. |

**Change 112:**

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.3 – Data Migration, **DELETE** APP-DM.04 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| APP-DM.04 | Support the GC with guidance and documentation in the migration of sample data and data validation. 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. |

**<u>Change 113:</u>**

**DELETE** ANNEX A, SECTION 3: TECHNICAL REQUIREMENTS in its entirety, and **REPLACE** with the following:

# 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 a solution based on the requirements, the High Level ISST Solution Conceptual Architecture and using the technologies listed in this statement of work. The Solution must be user friendly, reliable, maintainable, scalable, interoperable, extendable to accommodate the modification, adjustment, or addition of business process workflows, system automated functions, and compliant with GC IT/IM policies, guidelines and environment.

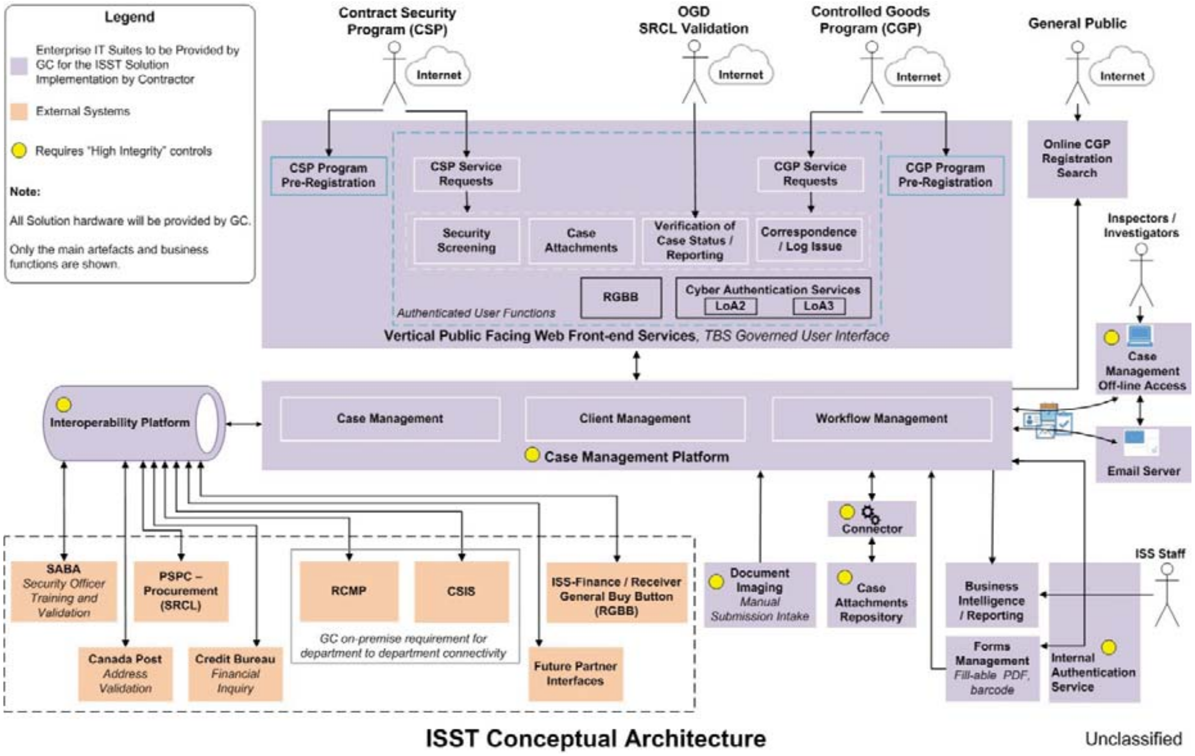

Legend
Enterprise IT Suites to be Provided by GC for the ISST Solution Implementation by Contractor
External Systems
Requires "High Integrity" controls
Note:
All Solution hardware will be provided by GC.
Only the main artefacts and business functions are shown.
Contract Security Program (CSP)
Internet
OGD SRCL Validation
Internet
Controlled Goods Program (CGP)
Internet
General Public
Internet
CSP Program Pre-Registration
CSP Service Requests
CGP Service Requests
CGP Program Pre-Registration
Online CGP Registration Search
Security Screening
Case Attachments
Verification of Case Status / Reporting
Correspondence / Log Issue
RGBB
Cyber Authentication Services
LoA2
LoA3
Authenticated User Functions
Vertical Public Facing Web Front-end Services, TBS Governed User Interface
Inspectors / Investigators
Case Management Off-line Access
Interoperability Platform
Case Management
Client Management
Workflow Management
Case Management Platform
Email Server
Connector
SABA Security Officer Training and Validation
PSPC – Procurement (SRCL)
RCMP
CSIS
GC on-premise requirement for department to department connectivity
ISS-Finance / Receiver General Buy Button (RGBB)
Canada Post Address Validation
Credit Bureau Financial Inquiry
Future Partner Interfaces
Document Imaging Manual Submission Intake
Case Attachments Repository
Business Intelligence / Reporting
Forms Management Fill-able PDF, barcode
Internal Authentication Service
ISS Staff
ISST Conceptual Architecture
Unclassified

**Figure 2:** High Level ISST Solution Conceptual Architecture

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.

External Users, such as Contract Security and Controlled Goods Program applicants, will access the functionality required for their business processes via the Vertical Public Facing Web Front-end Services. These users will gain access to the environment after being authenticated at the appropriate level of assurance required by the application using the cyber authentication services and based on defined roles and rights. There will be **no** direct access to the MS Dynamics CRM core platform by External Users. The Vertical Public Facing Web Front-end Services platform will host web enabled forms for the requisition of and receipt of services. The configuration of Vertical Public Facing Web Front-end Services enabling business intake processes interfaces must meet GC requirements (WCAG) for web standards.

The Contractor will configure technology that will reside on the GC network, interface with the Dynamics CRM Case Management Platform, be scalable to meet future growth, use web services, and predominantly leverage configuration over customization.

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.

The Solution must leverage PWGSC identified technology in the descriptive list below. These technologies are Enterprise IT Target Suites that are driven by the Chief Information Officer Branches (CIOB) of TBS or PWGSC, in order to reduce and streamline the application footprint for GC and PWGSC applications. Wherever possible, the Contractor must meet the requirements of the Solution, including any new requirements driven by business process re-engineering through leveraging these technologies to build a unified Solution.

The identified Enterprise IT Target Suites that the Contractor must adhere to include, but are not limited to:

(a) **Dynamics CRM (On premise) 2015 (or higher) (Enterprise IT Target Suite)**
**Case Management Technology** - The Vertical Public Facing Web Front-end Services for business intake 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.

(b) **Microsoft Exchange Server, Outlook Client (Enterprise IT Target Suite) and MS Dynamics CRM for Outlook GC e-mail** – This technology will be used to support e-mail and off-line Case Management capabilities for internal users such as field inspectors.

(c) **SAP Business Objects (Enterprise IT Target Suite)**
**Business Intelligence Reporting** - SAP Business Objects BI 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 BI connected to a PureData warehouse. Reporting functionality must be available to both Internal and External users based on the users' application profiles.

(d) **Oracle Service Bus (Enterprise IT Target Suite) Information Sharing Technology** - GC Interoperability Platform (GCIP – based on Oracle Service Bus (technology). Information sharing between ISS and partner organizations should be automated and managed in accordance with GCIP capabilities and the underlying Oracle Service Bus technology.

(e) **Imaging/Scanning System -** This system is in place and uses IBM DataCap technology. The ISST Solution will need to exchange information with this system.

(f) **Documents and Records Management System -** The Solution is expected to require the storage, management and retrieval of data largely grouped into two categories: (1) Database or Data Management System - processing-intensive, higher transaction structured data typically associated with in-process requests and with company and personnel data, and (2) Document and Records Management System – unstructured data typically associated with attachments that should not be altered but must be retained for document & records management and evidentiary purposes (e.g. passports, birth certificates etc.), representing low transaction, infrequent retrieval rate processing.

i) **Database or Data Management System -** The Contractor must leverage existing products already licensed and in use by PWGSC, to satisfy the requirements for non-sensitive, sensitive, and intensive information/data processing purposes.  The Solution should use the GC standards of SQL Server/Oracle for any database applications.

ii) **Documents and Records Management System -** The current GC standard for document and records management is OpenText Content Server, which should be leveraged for unstructured data long-term storage. This would be the default for items which are not required for dynamic processing, and includes (but is not limited to)  static attachments and manually submitted forms that are digitized for document and records management purposes.

The Contractor must provide IM/IT technical expertise in the areas of application development particularly configuration and integration of various technology platforms as outlined in this statement of work; 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, 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 | Enables and implements 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. |

| SOW NUM | Requirement |
|---|---|
| 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 | Enables and implements automatic termination of an open web session after a period of inactivity as determined by GC. |
| Tech.06 | Enables and implements 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:<br>(a) PDF (Adobe PDF);<br>(b) DOC, DOCX (MS word 2013 and above); and<br>(c) XLS, XLSX (MS Excel 2013 and above). |
| Tech.07 | Implements the Solution for supporting 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 | Implements the Solution 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). |
| 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 | Implements 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 | Implements 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 Vertical Public Facing Web Front-end Services to enable business intake processes such as creating web enabled forms to gather and exchange information, and that 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. |

| SOW NUM | Requirement |
|---|---|
| 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 the applicable “Protected B, High Integrity, Medium Availability” (PB/H/M) security profile requirements for the platforms as identified on the ISST Conceptual Architecture diagram. |
| Tech.18 | Ensures conformance with the GC Web Standards (https://recherche-search.gc.ca/rGs/s_r?cdn=canada&st=s&num=10&langs=en&st1rt=1&s5bm3ts21rch=x&q=web+standards&_charset_=utf-8&wb-srch-sub=) and Web Accessibility (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601) requirements for the Vertical Public Facing Web Front-end Services enabled business intake processes. |
| 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. |
| 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:<br>(a) Near Real-Time or batch;<br>(b) Web services / APIs;<br>(c) XML and/or Flat file;<br>(d) Export and import of data and content; and<br>(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 and supports GC and IT industry best practices and standards that have been adopted widely for building and maintaining a high-performing IT system to:<br>(a) Provide easy-to-use Web applications;<br>(b) Ensure and maximize the maintainability of the Solution;<br>(c) Ensure and achieve high level reliability;<br>(d) Ensure scalability and sustainability; and<br>(e) Deliver acceptable system performance. |

| SOW NUM | Requirement |
|---|---|
| Tech.27 | Supports GC's strategic plans for application interoperability, including, at a minimum by:<br>(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<br>(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.<br>The following is a list of types of expected technologies that must be supported:<br>(a) SAML 2.0<br>(b) JSON<br>(c) Kerberos<br>(d) X.509<br>(e) LDAP<br>(f) RBAC<br>(g) OAuth<br>(h) SOAP<br>(i) REST<br>(j) oData |
| Tech.29 | Supports, uses and/or develops structured and modular external interfaces which allow information exchange between the Solution and other systems through a secure communications infrastructure.<br>These interfaces include, at a minimum:<br>(a) An intranet or extranet for the business processes described in "Section 2: Business Requirements";<br>(b) Web services – third party data feeds;<br>(c) Commercially available third party security components such as Public Key Infrastructure (PKI) products; and<br>(d) GC or NGO systems containing supporting information needed to process transactions. |
| Tech.30 | Interoperates with other systems and platforms, as indicated in Figure 2, using as a minimum the following:<br>(a) APIs;<br>(b) Export and import of data and content; and<br>(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 ISST Logical and Physical architecture blueprints (using GC templates) based on the ISST Conceptual architecture blueprint. These blueprints are subject to GC approval. |
| 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. |
| Tech.36 | Design and create a data architecture which:<br>(a) Includes all appropriate data models, specifically, conceptual, logical, and physical;<br>(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;<br>(c) Includes data dictionaries;<br>(d) Will operate within the ISS Solution environment;<br>(e) Supports all ISS business processes; and<br>(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:<br>(a) Concept of Operations;<br>(b) Systems Overview;<br>(c) Interface Overview (for every Interface in, to and from the application);<br>(d) Functional Allocation;<br>(e) Data Transfer;<br>(f) Transactions;<br>(g) Security and Integrity;<br>(h) Detailed Interface Requirements;<br>(i) Interface Processing Time Requirements;<br>(j) Message (or File) Requirements;<br>(k) Communication Methods;<br>(l) Security Requirements;<br>(m) Qualifications Methods;<br>(n) Approvals; and<br>(o) Record of Changes. |

| | |
|---|---|
| Tech.39 | Provide a Solution that allows for the management of forms via configuration in Dynamics (or another means) without the need of a developer. |
| Tech.40 | Design the Solution to ensure that “digital signatures” are used for both, internal user and internal service initiated processes where required. |
| Tech.41 | Identify and describe, within their physical architecture design, the security controls to be implemented by the Contractor, and the GC. |
| Tech.42 | Define the contents for and configure the Solution to produce system generated audit files to include information to facilitate integrity violations determination. |
| Tech.43 | Configure the Solution to enforce user account restrictions (e.g. time of day, day, week, etc.) |
| Tech.44 | Create a process that will store previous configurations of the Solution to support version rollback for a period to be defined by the GC. |
| Tech.45 | Configure the Solution to prevent unauthorized and unintended information transfer via shared system resources. |
| Tech.46 | Configure the Solution to respond automatically when integrity violations occur. |
| Tech.47 | Configure the Solution that meets the requirements of the current solicitation. |
| Tech.47.A | Provide Detailed Design Specifications |
| Tech.47.B | Provide a Relationship Management Approach, including the following elements:<br>(a) Overall approach to Government of Canada and Contractor relationship management;<br>(b) Communications between the Government of Canada and the Contractor in respect to a proposed governance model and team structure as detailed in R1. A.;<br>(c) Issue management and resolution;<br>(d) Joint planning and managing of changes to project scope and schedule |

The Contractor must utilize Vertical Public Facing Web Front-end Services for business intake technology that:

| | |
|---|---|
| Tech.48 | Installs and operates on a Windows 2012 server platform, and Internet Information Services (IIS) web server. |
| Tech.49 | Leverages predominantly, configuration vs. customization. |
| Tech.50 | Resides on the GC network and is scalable. |
| Tech.51 | Is configured to allow Government of Canada Credential Federation (GCCF) Credential integration. |
| Tech.52 | Interfaces/integrates with MS Dynamics CRM (2015 or later) using web services and/or other approved and supported methods by the underlying technology platforms for its integration with Dynamics CRM Case Management Platform. |

| | |
|---|---|
| Tech.53 | Supports content creation and publishing in Canada’s official languages – English and French. |
| Tech.54 | Supports wireless and mobile devices. |
| Tech.55 | Supports encryption. |

**Change 114:**

At ANNEX A, SECTION 4: SECURE ACCESS, under 1.2.2 – External Users, **DELETE** SecureExt.02 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| 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 Vertical Public Facing Web Front-End Service. |

**Change 115:**

At ANNEX A, SECTION 5: IT SECURITY REQUIREMENTS, 1.2 – Detailed Requirements, under the category Access Control and Account Management, **INSERT** the following:

| | |
|---|---|
| SC.00.A | The Contractor must prepare a User Access Control and User Management Plan. |

**Change 116:**

At ANNEX A, SECTION 5: IT SECURITY REQUIREMENTS, under 1.2 – Detailed Requirements, **DELETE** SC.48 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| SC.48 | The Contractor must provide detailed Security Installation Procedures to GC that include, at a minimum:<br>(a) Steps necessary for the secure installation and configuration;<br>(b) Installation and configuration of all technical security solutions;<br>(c) Security configuration of Hardware products; and<br>(d) Security configuration of software products. |

**Change 117:**

At ANNEX A, SECTION 6: TESTING MANAGEMENT, 1.2 – Detailed Requirements, under the category Test Management (General):

**INSERT** the following:

| | |
|---|---|
| TM.00.A | Prepare a Preliminary Testing Plan in accordance with the requirements of ANNEX A, Section 6. The Contractor should be guided by the business and technical requirements and conceptual architecture for preparing the test plan. |

**DELETE** TM.01 in its entirety and **REPLACE** with the following:

| | |
|---|---|
| TM.01.A | Before commencement of the development Work, the Contractor must develop the Testing Strategy. Subject to the approval of the Project Authority, the Strategy must include, as a minimum but not limited to, the following information for all stages of the required testing:<br>(a) A high-level of overview of the proposed testing strategy;<br>(b) A Defect Management Framework;<br>(c) Entry and exit strategy;<br>(d) Meetings between the Contractor and Project Authority; and<br>(e) On-going risk management and mitigation strategy. |

| | |
|---|---|
| TM.01.B | The Contractor must develop a Testing Plan which demonstrates, but is not limited to:<br>A. Due consideration of related Security requirements from SC-42 Security Integration Test Plan as well as Section 6 of ANNEX A;<br>B. Adequate test coverage to ensure Solution go-live readiness. Due consideration of and reference to :<br>i. Integration testing;<br>ii. Functional and non-functional Testing, including Security Testing;<br>iii. Data Validation Testing;<br>iv. Client acceptance testing.<br>C. The identification of risk and its management. |

**INSERT** the following:

| | |
|---|---|
| TM.06.A | Provide the completed Requirements Traceability Matrix. |

**Change 118:**

At ANNEX A, SECTION 7: MANAGEMENT AND OVERSIGHT, 1.3 – Detailed Requirements – Project Management, under the category Project Plan (General):

**DELETE:**

| | |
|---|---|
| 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. |

**INSERT:**

| | |
|---|---|
| PM.05.A | The Contractor must prepare a Preliminary Project Management Plan that reflects their 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. |
| PM.06 | 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.<br>The Plan must respond to the following requested elements and indicate how they support the intended outcomes listed in ANNEX A, Section 1 and 7, including:<br>(a) Project Governance and Team Structure Document;<br>(b) Scope Management Plan;<br>(c) Schedule Management Plan;<br>(d) Project Schedule;<br>(e) Risk Management Plan; and<br>(f) Quality Management Plan. |

**Change 119:**

At ANNEX A, SECTION 7: MANAGEMENT AND OVERSIGHT, 2.2.2 Change Management Plan, under the category General:

**DELETE:**

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

**INSERT:**

| | |
|---|---|
| CM.01.A | The Contractor must prepare a Preliminary Change Management Plan which includes, but is not limited to:<br>A. A comprehensive understanding of the Change Management requirements;<br>B. Consideration of the following:<br>i. Avoidance of disruption of service to Canadians;<br>ii. Facilitation of the adoption of process and terminology transitions for all end users, including external users and internal staff;<br>iii. Appropriate, accurate and timely use and input to the new system; and<br>iv. The quality and integrity of the services rendered.<br>C. A comprehensive evaluation method for assessing effectiveness of change management activities. |
| CM.02 | The Contractor must prepare a Change Management Plan after the Preliminary Change Management Plan has been evaluated by Canada and deemed that the plan supports the successful transition from “as-is” to “to be” states and demonstrates the requirements identified above.<br>The Change Management Plan must be integrated with the Project Management Plan and Project Schedule. |
| CM.03 | The Contractor must:<br>(a) Develop processes and procedures to institutionalize the change;<br>(b) Identify change management activities and link them to project milestones;<br>(c) Align with training timelines, communications, and approaches;<br>(d) Align with process re-engineering transition activity timelines; |

| | |
|---|---|
| | (e) Identify change resourcing expectations based on project phases and milestones;<br>(f) Identify when, for how long, and the type of GC resources that are required for change management;<br>(g) Identify high risk areas that might impact successful change, develop mitigation strategies and recommended mitigation actions, and report results to GC;<br>(h) Identify quick wins for simplifying change management activities;<br>(i) Work in collaboration with the GC in executing the Change Management Strategy and Plan;<br>(j) Action change management remediation activities required throughout project lifecycle;<br>(k) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues;<br>(l) Support identified GC Change Management resources who will champion change;<br>(m) Coordinate between the various components of change management and the other project activities; and<br>(n) Provide an in service support plan which includes knowledge transfer for operations. |

**Change 120:**

At ANNEX A, SECTION 9: OPTIONAL SERVICES, **INSERT** the following:

## 1.8 ADDITIONAL SECURITY SERVICES

In addition to the Security services described in Section 5: IT Security Requirements, the Contractor must, on an as-and-when basis, provide additional IT Security services and must propose resources that are qualified and have experience providing IT Security services.

**Change 121:**

At Appendix 2 to ANNEX A – Key Activities, **DELETE** the schedule of Key Activities in its entirety and **REPLACE** with the following:

| Key Activities | Completion Date |
|---|---|
| Contract Award | August 2017 |
| Solution 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 |

**Change 122:**

At Appendix 2 to ANNEX A – Key Activities, **DELETE 9. Stabilization and Transition-Out** in its entirety and **REPLACE** with the following:

**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 Report:
- Assessment of project performance;
- Identification of lessons learned;
- Confirmation that essential contractual and other project closure activities have been completed;
- Outstanding Issues;
- Transfer of assets, deliverables and ongoing administrative functions; and
    - Measurement of post implementation benefits/outcomes (KPI) delivered by the project.

(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.

**Change 123:**

At Appendix 3 to ANNEX A – User Accounts Overview, under 1. External Users:

**DELETE:**

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.

**INSERT:**

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 Vertical Public Facing Web Front-end Service.

**Change 124:**

At Appendix 5 to ANNEX A – Glossary of Terms:

**DELETE:**

**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 System Data:** I) service delivery portal

**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.

**INSERT:**

**Intuitive interface:** Solution interfaces that are intuitive, as defined above (“Intuitive”), for both the Vertical Public Facing Web Front-end Service and Services Processing Application portions of the Solution.

**ISS System Data:** l) service delivery Vertical Public Facing Web Front-end Service

**Vertical Public Facing Web Front-End Service:** 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 Vertical Public Facing Web Front-end Service include intranet "dashboards" for executives and managers.

**Change 125:**

**DELETE** ANNEX B – Price Schedule in its entirety and **REPLACE** with the ANNEX B – Price Schedule attached to this Amendment.

**Change 126:**

**DELETE** ANNEX F – Resource Category Information for Optional Services in its entirety and **REPLACE** with the ANNEX F – Resource Category Information for Optional Services attached to this Amendment.

**Change 127:**

**DELETE** Attachment 1 to Part 4 – Technical Evaluation in its entirety and **REPLACE** with the Attachment 1 to Part 4 – Technical Evaluation attached to this Amendment.

**Change 128:**

**DELETE** Form 3 to Part 4 – Bid Solicitation – Financial Bid Form in its entirety and **REPLACE** with the Form 3 to Part 4 – Bid Solicitation – Financial Bid Form attached to this Amendment.

## B. QUESTIONS

**Question 164:**

Please clarify the boundaries of what is provided by the SCMS service and SSC as it relates to the requirements in Annex A – Statement of Requirements, 1.2 Detailed Requirements in terms of areas including:

a) Configuration Management
b) Boundary Protection and Security
c) Monitoring

**Answer 164:**

The following is clarification of what is provided by the CIOB and SSC as related to the requirements in ANNEX A – Statement of Requirements, 1.2 Detailed Requirements:

a) CIOB handles the configuration management for the Dynamics platform. The CIOB will provision tenants on the shared Dynamics platform for the Contractor’s implementation of the Solution. SSC will be responsible for the infrastructure aspects of the ISST Solution, such as virtual machines, storage, and networking. The PWGSC IT Project team will coordinate the Contractor's Solution implementation activities with both SSC and CIOB.

b) Boundary Protection is part of the security response to the overall security requirements for the Solution. Boundary Protection in this context is associated with the IT infrastructure which is delivered by SSC, and therefore, SSC is responsible for that component.

c) Monitoring is required for two aspects of the Solution; 1) Performance – CIOB and SSC collaboratively monitor the MS Dynamics platform health in order to troubleshoot issues or potential issues such as scaling. 2) Security - monitoring is a security requirement for the purposes of data integrity at the application level. The Contractor will be responsible for any ISST Solution (application level) monitoring required.

**Question 165:**

What are the responsibilities of the bidder and what is already being provided from SCMS and SSC that bidders can leverage?

**Answer 165:**

The Contractor is responsible for all software configurations, development, and integrations of the ISST Solution using the provided platforms and services in accordance with the Statement of Work.

Shared Services Canada (SSC) is responsible for delivering and supporting infrastructure, such as servers, networking and email.

- All solution hardware of the solution platform including servers and network connectivity etc. will be provided by GC
- All IT Target Suites will be provided by GC.

CIOB delivers the Case Management capabilities using MS Dynamics CRM technology platform based on a multi-tenancy architecture.

The CIOB service includes:

- MS Dynamics infrastructure for non-production and production
- Administration and support of the shared platform
- Dynamics license management
- Federated Security model allowing for easier integration into GC wide systems
- Platform accreditation for Protected B sensitivity of data with medium availability and integrity
- Performance and problem monitoring on the platform with auto notifications
- Patching
- Platform scaling on-demand
- Tenant resets and data backups
- Development best practices and guidance
- On-boarding and coordination of Dynamics integration flows with SSC

**Question 166:**

If products other than those in the "GC packaged inventory" are recommended by a bidder how bidders should reflect the license costs for these additional products in their proposals?

**Answer 166:**

Please see the response to Question 204 in this Amendment 011.

**Question 167:**

PSPC indicates on page 32 of ANNEX A – Statement of Work that “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.” Is it accepted that if such a product is not approved post contract award this will represent a change request for replacement?

**Answer 167:**

Please see the response to Question 204 in this Amendment 011.

**Question 168:**

The RFP, including the Security Requirements Check List (SRCL), seems to allow for bidders and their subcontractors from outside of Canada to bid on or be involved in this competition. This seems to be directly at odds with current Treasury Board policy and practice for data sovereignty, especially where sensitive Government and citizen data is involved, e.g. personal security clearance background data, holding all the Government of Canada Secret and Top Secret clearances for Canadian industry, and processing sensitive Controlled Goods and Export Control information.

There is a potential for sensitive personal background data of Canadian citizens to be placed at risk, even if the supplier(s) are not operating the systems, but have an intimate technical knowledge of the systems used to process, store and safeguard that data. When aggregated at the national level across all the functional areas outlined in the Issue statement above, CGI believes that this aggregates to a substantial national security concern (e.g. how many and which people are cleared to the Top Secret level, and which subcontractors are approved to work on what classified contracts, for what departments).

It is strongly recommended that, consistent with other recent similar practices, that Canada impose national security exclusions for this requirement as follows:

a) All bidders, partners, or members of a Joint Venture must be registered in good standing in the Government of Canada Foreign Ownership, Control or Influence (FOCI) program;
b) Subcontractors continue to be approved individually consistent with the Government of Canada Subcontractor security program, taking into account the security exclusions in this RFP;
c) Products be reviewed for consistency with the Canadian Supply Chain Integrity policy; and
d) That bidder support for systems and services provided (e.g. 2nd and 3rd level) be restricted to personnel from within Canada, cleared to a level consistent with the SRCL unless specifically approved as an exception by PSPC.

**Answer 168:**

With respect to a), b), c) and d), please see the response to Question 5 in Amendment 003.

**Question 169:**

In reference to Annex A, Section 4: Secure Access, 1.2 Detailed Requirements, 1.2.2 External Users, SecureExt.01 (page 38 of 70); can you provide the integration specification for the use of GCKey and Secure-Key Concierge?

**Answer 169:**

Integration specifications for the use of GCKey and Secure-Key Concierge can be found in the CATS2 document attached to this Amendment 011. It is expected that the infrastructure for the Vertical Public Facing Web Front-End Services and integration with GCCF will be in place using the current service (Active Directory Federation Services (ADFS)).

**Question 170:**

For SC.59 Information Flow Enforcement:

In an enterprise environment, like that of the Government of Canada, information flow enforcement is typically enforced at the security perimeter by a product that has the capability to analyze and adjudicate content of all content types in order to determine acceptability and also to detect malicious code (which could also entail manual adjudication by some groups responsible for assessing what is and is not acceptable):

a) Is it the intent of this requirement that the vendor propose this type of product as an additional element of the ISST Solution architecture or, rather, should the vendor assume that this type of platform is provided by the government as Government Furnished Software and is operated by SSC?
b) If the latter, then should the vendor also assume that the requirement is to provide support to SSC in their configuration of the Government's platform that monitors and supports information flow enforcement?
c) If the former, how should the vendor include the new product? Assume it can be inserted into the overall government infrastructure on the periphery of the environment and that the government will provide a team that can operate this platform? Address violations and perform manual adjudications where required?

**Answer 170:**

As per Tech.34, the Contractor must develop the physical architecture. This will include the interfaces to all known included components, third party partners etc. (details of interface requirements are in Tech.38)

a) The Contractor will be responsible for only those security controls implemented within the Solution software, and all supporting procedures that are within the Contractor's project scope. The Contractor will conduct a gap analysis as upon contract award and provide recommendations to the GC. The Contractor will be required to assist in the implementation and configuration of all Solution software.

b) The Contractor will be required to provide support to the GC in their configuration of any GC platform that is part of the ISS Solution physical architecture.

c) For further information, please refer to the response to Question 204 in this Amendment 011.

**Question 171:**

PSPC requires in SC.23 Information System Monitoring that:
"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."

At the same time on page 57 of "ANNEX A – Statement of Work" PSPSC indicates:
"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;"

We seek clarification to the role of SSC in implementing SC.23. Given that SSC is responsible for the specialized network infrastructure capable to implement the security functions described in SC.23, is the Contractor required to collaborate with SSC to ensure this infrastructure supports and integrates with the Solution or is the Contractor required to duplicate in the Solution the functions provided by SSC?

**Answer 171:**

The Solution's design must include the Information System Monitoring identified in SC.23. The Contractor must include this as a part of the Logical and Physical Architectures as described in requirement Tech.34. These architectures are to be built based on the ISST Conceptual Architecture and will have the specifications for all components of the ISST Solution platforms and services. PWGSC will provide support to the Contractor by facilitating access to required information that is out of reach to the Contractor and is required by the Contractor to complete deliverables.

**Question 172:**

In reference to ATTACHMENT 1 TO PART 4 – TECHNICAL EVALUATION, 3. MANDATORY CRITERIA, M1 contains the following volumetric requirement clause:

"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."

The volumetric data provides the following:

| User Type | CSP - Industry | CSP - Government | CSP Total | GSP Total | Accounts Total | 35% |
|---|---|---|---|---|---|---|
| Internal User Accounts | | | 396 | 91 | 487 | 170 |
| External User Accounts | 161,000 | 905 | 161,905 | 22,000 | 183,905 | 64,367 |
| Total Users | | | 162,301 | 22,091 | 184,392 | |
| | | | | 35% | 64,537 | |

a) In reference to Annex A – Statement of Work, Section 1: Canada's Industrial Security Solutions Overview, 3.1 Volumetric Data (page 9 of 70) refers to internal and external user accounts, but does not explain the difference between "number of users" and "number of accounts". Should "number of users" and "number of accounts" be interpreted as being one and the same? If not, could PSPC please clarify the difference between the two?

b) Are we correct in our interpretation that the total "*number of users and number of accounts*" in referenced projects should be no less than 35% of both internal and external user accounts (i.e., 184,392 * 35% = 64,537 users)?

c) Given that we meet b) above (i.e., 64,537 internal and external users), is it also required to have 170 internal user accounts (487 * 35%) to qualify?

d) Given that we meet b) above (i.e., 64,537 internal and external users), is it also required to have 64,367 external user accounts (183,905 * 35%) to qualify?

e) Given that the project was designed, developed, implemented and turned over to the client for continuing operations prior to registration by users, the current number of registrations is not known since we no longer have access to the system. In addition, registration and transaction volume are the property of the client and are considered confidential making it impossible for us to provide the information. Would PSPC consider removing this requirement or allowing for some general estimates of anticipated or designed volume?

**Answer 172:**

As clarified in the response to Question 38 in Amendment 004, the bidder's referenced projects must meet 65% of the volumetrics identified in Annex A, Section 1, 3.1.

The Crown is willing to accept anticipated volumetrics that were used in design and development rather than confirming actual volumetrics used by the referenced project in a post implementation capacity. This is to say that if the solution was designed and developed to service an intended volume of users, number of transactions and diversity of transactions that meets the minimum volumetrics requested in M1 and M2, then this project can be used as a reference. Note that the anticipated volumes must have remained greater than the identified minimum volumetrics throughout the duration of the project.

Please refer to Change 127, and Questions 202 and 216 in this Amendment 011.

**Question 173:**

In reference to ATTACHMENT 1 TO PART 4 – TECHNICAL EVALUATION, 3. MANDATORY CRITERIA, M2 contains the following volumetric requirement clause:

"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."

a) Could PSPC clarify in detail what is required to qualify for "Number of Transactions"? Are these referring to registration transactions or application transaction volume?

b) Could PSPC clarify in detail what is required to qualify for "Diversity of Transactions"? What would be the qualification criteria for another application that is similar, but not exactly the same as PSPC's? How can a different application dealing with different case types be shown to meet this "Diversity of Transactions" criterion? Would a list of CRM case types be sufficient? How will this be evaluated? In many cases, the transaction volume is not known to us given that after a successful implementation we no longer have access to the system. In addition, transaction volume is the property of the client and in many cases is considered confidential, making it impossible for us to provide this information. Would PSPC consider removing this requirement or allowing for some general description of anticipated volume?

**Answer 173:**

Diversity of transactions refers to different lines of business that are addressed within the same solution. These business lines may differ across various stakeholder groups, types of workflows managed or activities conducted, etc.

Please refer to Change 127, and 172, 202 and 216 in this Amendment for additional information regarding the provision of volumetrics.

**Question 174:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.01 (Page 41 of 70), (a) Enforce role-based access controls for all individual users.

Does Canada wish the bidder to provide a wholly contained role-based access controls (RBAC) or directory system (e.g. Active Directory), or is it intended that the bidder's solution would leverage Canada's existing RBAC and directory systems?

**Answer 174:**

The Contractor is expected to configure the Solution to provide role based access controls (as indicated in APP-OPS.01), leveraging existing internal GC directory services where and when necessary, rather than creating additional directories. The Contractor will determine what requirements can be met with existing directory infrastructure for external users.

**Question 175:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.09 (page 43 of 70).

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.

Question/Comment:

a) The bidder has no knowledge or responsibility for network architecture in the host environment or data flows and security capabilities external to provided solution. Will Canada consider amending the requirement to read as follows: Fully document any connections between IT systems, including data descriptions, data flows, security and access requirements and mechanisms, performance, and reliability expectations internal to the provided solution, as well as any external security or system dependencies?

b) The service provider is not the operator of the solution, or its host environment and, therefore, has no control or visibility of external information system services. Will Canada please clarify this requirement so that it appears consistent with the bidder's scope, or remove it?

**Answer 175:**

In accordance with the Interconnectivity group of Business Requirements (APP-ICN.01 - .10), the Contractor is responsible to design, build and document the interfaces (Tech.38) to meet these requirements. While not responsible for the infrastructure, the Contractor will be responsible to develop and configure the conceptual architecture components for enabling the required business processes while ensuring that the appropriate related security controls have been considered and incorporated. PWGSC will provide support to the Contractor by facilitating access to required information that is out of reach to the Contractor and is required by the Contractor to complete deliverables.

**Question 176:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.11 (page 43 of 70).

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 the applicable security requirements.

The bidder is neither the operational security authority, operating authority, nor the operational change manager for the solution once delivered and live. Will Canada consider deleting this requirement?

**Answer 176:**

For the duration of the contract, any new software acquired to replace or augment software that has been configured or installed by the Contractor as part of the Solution will require validation. The Contractor will be required to analyze the products within the confines of a Development/Test environment prior to the release of the software into production. It is at this time that the Contractor will have analyzed, tested security functions and informed GC of any impacts or uncovered vulnerabilities of the software.

**Question 177:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.16 (page 44 of 70). 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.

The GC (not the bidder) is responsible for the architecture of the environment in which the application system is hosted. For that reason, it would be very difficult for the bidder to portray the many points required in a response to this requirement (e.g. any detailed aspects of the enterprise architecture). It is recommended that bidders be required to provide a proposed high-level security architecture/topology, with narrative annotations, showing how the bidder's system would be deployed and secured in an enterprise architecture that is consistent with GC standards (e.g. ITSG-22, ITSG-38, etc.) After contract award, the bidder can provide a more detailed application-level security architecture that addresses security integration within the host enterprise environment, as long as those details are provided at that time by the GC.

Will Canada consider amending this requirement as per the above recommendation?

**Answer 177:**

The Contractor must meet the requirements of SC.16, post contract award. In post contract circumstances where GC information is not readily available, the GC will assist the Contractor in obtaining the required information. There is no requirement to produce any Information Security Architecture (ISA) type documentation (other than for R4) prior to award.

**Question 178:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.17 (page 44 of 70). 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.

This requirement has the potential to be interpreted significantly beyond the scope of the bidder. It is recommended that it be amended to state "within the scope of the solution" in order to more clearly define the scope boundary.

Will Canada consider amending this requirement as per the above recommendation?

**Answer 178:**

As stated in the response to Question 170 in this Amendment, the Contractor must provide a physical architecture as part of the deliverables. That architecture must have the specifications for all components of the Solution. The Contractor must develop the Security High Level Solution Design (SHLSD) based on the physical architecture focusing on the solution scope allocated to the Contractor.

**Question 179:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.17 (page 44 of 70). 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 flow**s;
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.

As per SC.17, the bidder is only responsible for the provision of a secure application/system. The security and design of the hosting environment is a GC responsibility. Although the bidder will need to advise on secure/appropriate placement and interfaces, the bidder should not have primary responsibility for the following, but should only support:

- Enterprise security architecture;
- Operational security management;
- Patch management; or operational change management.

It is recommended that this requirement be re-scoped to reflect the observations. Where appropriate, the bidder can advise on those elements, but not be responsible for out of scope elements. Will Canada consider amending this requirement to clarify which items the Bidder is responsible for and which items the Bidder is required to support?

**Answer 179:**

The Contractor will be responsible for controls implemented within the Solution software, and all supporting procedures. Where the Contractor is unable to apply a control, the Contractor will assist the GC in its implementation and documentation.

Regardless of which controls the Contractor must implement, it is their responsibility to document all controls during design of the physical architecture which includes all components of the entire Solution. The SHLSD supports and informs the architecture as it identifies all security controls and where they are applied.

The SHLSD also supports the development of the SDSD (requirement SC.18), which contains the detailed information of the security controls for the Contractor provided Solution components.

The physical architecture, the SHLSD and the SDSD are all within the scope of the Contractor's work and will be supported by the GC.

**Question 180:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.18 (page 44 of 70). 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.

Refer to observations at question 98. The diagram required is usually described as a network-centric, layer 3, Security Topography diagram, with a document that provides annotated descriptions of how all security-related constructs and safeguards, including how all technical security requirements are to be fulfilled.
Will Canada consider amending this requirement to clarify which items the Bidder is responsible for and which items the Bidder is required to support?

**Answer 180:**

The Contractor must produce a Security Detailed Solution Design (SDSD) from the Security High Level Solution Design (SHLSD) (SC.17) for the Solution as designed by the Contractor. The SDSD must reference all the related security controls for the designed solution. Please refer to the responses to Questions 170 and 178 in this Amendment for additional information.

**Question 181:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.19 (page 45 of 70). 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.

Certain traffic filtering and other discriminatory safeguards can be implemented on the solution. However it will also be dependent upon enterprise firewalls, IDS and other systems designed and operated by the operating environment authority and the security management authority (SSC).

Will Canada consider amending this requirement to clarify which items the Bidder is responsible for and which items the Bidder is required to support?

**Answer 181:**

During the creation of the physical architecture, the Contractor will provide integration specifications for devices that are part of the design but are considered to be outside the scope of the Contractor supported Solution. The Contractor must, when creating the architecture, take into consideration the security control requirements and indicate where they should be implemented. If the Contractor determines that to satisfy security control requirements, additional components should be added to the Solution, then it is expected that the Contractor will provide a recommendation and will implement those controls once approved by the GC. The Contractor will be responsible to support or assist the GC in supporting the Solution for the duration of the contract.

**Question 182:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.20 (page 45 of 70). The Solution must fail securely in the event of an operational failure of a boundary protection device.

This is normally the default setting for all firewalls and security-aware boundary devices. As such, most of the systems this applies to would be provided by the GC (e.g. zone and PAZ firewalls, etc.). The only exception would be any host-based firewalls internal to the Solution.

Will Canada consider deleting this requirement or amending to clarify the responsibility of the Bidder?

**Answer 182:**

The requirement is that the Solution fail securely in the event of a boundary protection device. The Comment/Question states that this is the default setting for most boundary devices. That is not the required control. The Contractor must ensure that the Solution (that which is constructed by the Contractor) fails securely.

**Question 183:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.23 (page 45 of 70). 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.

This should be the responsibility of the operations and security operating authorities.

The bidder can work with the operations and security operating authorities to ensure that appropriate detection and monitoring capabilities are included. However, it is beyond the bidder’s scope to monitor and notify. Will Canada consider deleting this requirement or amending to clarify?

**Answer 183:**

The Contractor will work with the GC to ensure that appropriate measures have been put in place to monitor and detect incidents. Note that SC.23 specifies that it is the Solution which must be able to notify security administrators.

Regarding the Contractors obligations to report security and privacy incidents, as per SC.33, the Contractor is responsible to notify the GC through the creation of a security incident ticket.

**Question 184:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.26 (page 46 of 70). 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.

Providing verbatim firewall rules will depend on the type of boundary devices employed by the operating authority. Usually, flow descriptions including origination, destination, port/protocols, encryption, etc. are provided. The firewall policies are then based on that. Will Canada consider amending the requirement or providing the above information?

**Answer 184:**

The Vertical Public Facing Web Front-End Services Solution platform and any associated firewalls will be configured by SSC as part of their infrastructure provisioning and support services. The Contractor is responsible to present the design for the Vertical Public Facing Web Front-End Services, required permissions and firewall requirements including ports and protocols to SSC for implementation upon approval.

**Question 185:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.37 (page 47 of 70). The Contractor must for the duration of the contract create one or more incident tickets for each incident detected.

The bidder is not responsible for security monitoring of the solution once it is operational. Will Canada please clarify what is meant by this requirement?

**Answer 185:**

Incidents subject to SC.37 may or may not occur from within the Solution software and/or be identified by reviewing log files. For the duration of the contract, any process or activity including user interaction which produces a situation contrary to the intended result will require an incident ticket. When the ticket has been created, the Contractor will be required to investigate any incident associated with the Contractor prepared

Solution. In cases where the Contractor does not have access, they will work with the GC to determine the cause.

**Question 186:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.38 (page 47 of 70). 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.

The bidder is not responsible for security monitoring of the solution once it is operational. Will Canada please clarify what is meant by this requirement?

**Answer 186:**

The Contractor is expected to monitor the Solution for the duration of the contract, this includes but is not limited to reviewing of log files for unexpected activity. Should new threats, vulnerabilities or incidents be uncovered, reported, or identified by the publishers of the software used in the Solution, or the business client or the Contractor, the Contractor is expected to assist the GC in assessing the risks to the Solution from the threats/vulnerabilities. This includes compliance with SC.37 as required.

**Question 187:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.39 (page 47 of 70). 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.

This is normally the responsibility of the IT operating authority in coordination with the security authority. Solution vendors can provide supporting advice and inputs as per SC.36.

Will Canada please clarify and adjust the requirement, as per SC.32, 33, 34, 36, 37, and 38?

**Answer 187:**

The solution vulnerability assessment must occur during the development cycle of the project, prior to production release. As per the response to Question 58 in Amendment 008, the Contractor will build the Solution from the physical architecture, detailing security controls within (detailed) and outside (high-level) the control of the Contractor. The Contractor will assist the GC in the vulnerability assessment within the limited project scope of the Contractor. The mitigation plan is required 5 days following the completion of the vulnerability assessment for any components that the Contractor is responsible for. Any mitigation of vulnerabilities may require the Contractor to work with the GC to complete. SC.36 references activities associated with incidents not vulnerability assessment.

**Question 188:**

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.70 (page 51 of 70). The Solution must implement multifactor authentication for network access to:

a) Privileged accounts; and
b) Non-privileged accounts.

Multi-factor authentication usually involves the issuance (and management) of hard or soft tokens in addition to a password. This can involve a certain amount of cost and is not usually used in the GC for public/non-privileged accounts.

Will Canada please confirm exactly which types of accounts/roles would require multi-factor authentication?

Will Canada please confirm that the ISST system would authenticate against a GC authentication system external to the application?

**Answer 188:**

Through business process reengineering, the Contractor is expected, to determine the authentication and access control requirements for each user role, based on the provided security controls for the PB/H/M security profile designation. See RFP Amendment 3, Controls IA 2, and IA 5 for additional information on access management. Refer to the response to Question 169 in this Amendment for additional details regarding authentication service requirements.

**Question 189:**

In reference to Data Structure:

Has a QUALITY evaluation been performed on the actual source data files? Since the Contractor will only be working with the sample data files, has the client recently performed any quality testing on the TRUE source data? If not, how long ago since the last quality evaluation was performed?

**Answer 189:**

Please see the response to Question 111 in Amendment 008.

**Question 190:**

Could PWGSC provide us with a copy of the BI architecture diagram showing all tables that currently exist (including their key structure)?

**Answer 190:**

There is currently no BI architecture available as the BI environment has not yet been established for the ISST project. Please see the response to Question 119 in Amendment 008 for further information.

**Question 191:**

What is the update frequency (refresh frequency) of the data warehouse and data marts?

**Answer 191:**

As there is no BI environment set up for the ISST project, these details cannot be provided at this time. Please refer to the response to Question 190 in this Amendment 011.

**Question 192:**

Could PWGSC provide the existing ETL jobs diagram (source to target) and what tool is used to execute these ETL scripts?

**Answer 192:**

Currently there are no ETL jobs diagrams to be provided as all current reporting is completed within the legacy business systems or through direct adhoc database queries. In assessing the ISST reporting requirements and potential identification of a need for a BI Solution, the Bidder will be expected to propose ETL scripts to maintain the BI data. For information regarding ETL tools please see the response to Question 67 in Amendment 006. However, please refer to the response provided at Question 204 in this Amendment 011 regarding procurement of software. For further information regarding the BI environment please refer to Question 190 in this Amendment.

In regards to data migration, the Contractor is expected to develop scripts to migrate data from the legacy data sources. Please refer to the data migration requirements located in Section 2 of ANNEX A.

**Question 193:**

SOW NUM SC.23 - Please confirm the Crown wishes the Contractor to provide attack detection and notification technologies in addition to existing PWGSC / SSC security technologies in place?

**Answer 193:**

The Contractor must leverage existing attack detection and notification technologies currently available within the GC and identify any areas where these technologies do not satisfy requirements.

Please refer to the response to Question 204 for additional information.

**Question 194:**

In Amendment #3, the Crown has changed the level of Integrity required by the Solution from Medium integrity to High integrity. This is a material change to the security controls requirements especially the level of automation required by the additional controls provided in this amendment. In addition, the Crown's response to question 18 states that contractors should not assume that existing information exchange channels comply with the security requirements. This material requirement change and answer raise, as the Crown is well aware, the level of risk of a more complex solution and potential delays involving numerous other stakeholders that may not be in a position to support such High integrity requirements.

During the bidder's conference the Crown advised that it's budget for this project was between $6-$11million, however, based on the Crown's revision of the Integrity profile of the solution, has the Crown also revised the impacts such a decision could have on its budget both from one-time costs and ongoing maintenance perspectives? If so, could the Crown advise the vendors of the change in budget?

**Answer 194:**

Canada has reviewed the requirements for the Total Firm Lot Price, and has revised the lower limit from $6,000,000.00 to $8,000,000.00. The upper limit remains unchanged. Please see Change 128 in this Amendment 011.

**Question 195:**

Regarding SC.19: The requirement states “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.” With respect to this requirement:

a) What are the ISS availability targets as they are not referenced in the RFP?
b) What are the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) criteria?

**Answer 195:**

In accordance with an ISS completed Business Impact Assessment (BIA) and Business Continuity Plan (BCP):

a) The target availability for the ISST is, the system must be available 99.35% of the time.
b) The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) criteria are 8-14 days (Tier 2) and 1 hour respectively.

**Question 196:**

As per Amendment 3, Change 39 (page 7 of 18), ANNEX A Section 5, under 1.2 now includes the statement that “The Contractor will be responsible to incorporate all security controls, including those met by PWGSC, SSC and the Contractor, in the Security Requirements Traceability Matrix.”

Question: Could Canada please clarify, as this has the potential to be an uncontrolled dependency/risk to the Contractor:

a) Will the Contractor be expected to populate the SRTM with explanations outlining how PWGSC and SSC are meeting the requirements of those controls that are not the Contractor’s responsibility? If so, how would the Contractor get that information in a timely manner?
b) Will the Contractor be indemnified from any compliance responsibility outside of its scope and control?
c) And If ATO is delayed due to SRTM non-compliance by SSC or PSPC (ie beyond the Contractor’s control), how will the Contractor be protected or compensated?

**Answer 196:**

The Contractor must include all security controls identified by the Contractor within the physical architecture into the SRTM document. The Contractor may not have in their possession, complete documentation from the GC with respect to the GC provided security controls, but that should be stated so within the SRTM.

a) The Contractor will provide explanations of their implemented security controls and insert any information available from PWGSC/SSC for controls outside the Contractor’s scope of implementation.
b) Canada will not indemnify the Contractor except where appropriate.

c) Please refer to the Standard Acquisition Clauses and Conditions Manual, 2035 - General Conditions – Higher Complexity – Services, article 10, Excusable Delay.

**Question 197:**

Will there be any further changes to Section 5: IT Security?

**Answer 197:**

Please see Changes 115 and 116 in this Amendment 011. No further changes are planned for Section 5 of Annex A for the duration of the RFP process. However, if changes are required, they will be communicated through formal amendment.

**Question 198:**

Requirement APP-IM. 27states: “Enables Internal Users to retrieve archived records from a case file for a specified period of time”.

Do “archived records” include records held in the legacy ISS system, and / or records held in partner systems (e.g. RCMP) that relate to a past case, or do they only include records held within the to-be solution (which would include those held in GCDOCS)?

**Answer 198:**

With respect to APP-IM.27, archive records do not include those held within the legacy ISS systems or partner systems that relate to a past case. They only pertain to records held within the To-Be Solution. For more detail on information the To-Be Solution will host, please refer to the response to question 88 in Amendment 007.

**Question 199:**

We hereby request that the question due date be amended to 5 days before bid closing.

**Answer 199:**

Canada will not amend item 2.3 of Part 2 of the RFP, Enquiries – Bid Solicitation.

**Question 200:**

Appendix 2 to Annex A – Key Activities – the schedule listed indicates both the “Planning and Analysis” and “Solution Design” as key activities. Several of our work streams (e.g. Testing or Training) cannot complete their Planning, Analysis and Design until after the solution itself is almost fully developed and implemented.

Can the initial “Planning and Analysis” key activity be renamed to be “Solution Planning and Analysis”? This would then exclude these downstream work streams from being required to complete early planning, analysis and design by Dec 2017 that, very probably, will have to be updated and re-reviewed in the latter half of 2018 after the solution is designed and almost completely developed.

**Answer 200:**

To provide clarity, as suggested the Key Activities has been amended to indicate “Solution Planning and Analysis”. Please refer to Change 121 in this Amendment 011. For further information regarding the Key Activities, please refer to the response to Question 154 in Amendment 009.

**Question 201:**

A large number of requirements in Annex A have changed. Can PSPC republish Annex A in its entirety reflecting the various amendments in order to ensure vendors’ responses address the most recent form of the requirements?

**Answer 201:**

ANNEX A has been updated to incorporate all changes to date, and is attached to this Amendment 011.

**Question 202:**

Attachment 1 to Part 4, M1; Amendment 004, Change 49– It is understood that Canada is seeking Bidders with specific Business Process Re-Engineering (BPR) and Change Management experience and expertise on large/complex projects. That said, the complexity of BPR and Change Management initiatives for large engagements is due to the change and resulting impact to Clients’ operational environment, as well as to their staff – not volumetric data.

It is requested that the volumetric data requirement for M1 be removed and replaced with a more relevant indicator of size and complexity, such as project dollar value.

Alternatively, it is requested that the volumetric data identified in Amendment 004, Change 49 be satisfied cumulatively by all the reference projects used in support of M1.

**Answer 202:**

Canada will be evaluating projects referenced by Bidders to ensure that they are similar in size and scope to the ISST initiative. The requested volumetrics in M1 and M2 provide a baseline for this assessment:

- By identifying the number Internal and External clients (accounts);
- By identifying the volume of transactions that pass through the provided solution (transactional volumes); and
- By identifying the different business lines captured (diversity).

Canada believes that an IT project encompassing the volumetrics requested provides a gaugeable indicator of the amount of change management and business process re-engineering activities that would have been required.

With regard to merging volumetric data from different projects, Canada does not feel that the requested volumetrics should be satisfied cumulatively across the reference projects and will not be making any changes to the Technical Evaluation in that regard.

However, M1 and M2 have been amended. Please refer to Change 127, and the responses provided to Questions 172 and 216.

**Question 203:**

Attachment 1to Part 4, M2; Amendment 004, Change 51– As identified at the Bidders Conference, Canada wished to leverage the expertise found in Industry to support this initiative. The experience that exists across the large system integrators, sought by Canada, has been gained across a number of diverse, large-scale, projects.

Canada's ask in M2 that all the reference projects each meet the volumetric requirements is restrictive and limits Bidders' ability to demonstrate their diverse, and otherwise relevant, experience. It is requested that the requirement be revised so that "at least one (1) of the three (3)" reference projects meet the volumetric data – which is consistent with the other components of M2.

Alternatively, it is requested that the volumetric data identified in Amendment 004, Change 49 be satisfied cumulatively by all the reference projects used in support of M2.

**Answer 203:**

Please refer to the response to Question 202 in this Amendment.

**Question 204:**

On April 28, 2017 we asked PSPC the following questions:

- As we review the requirements against the proposed solution architecture, we are seeing there may be gaps that will require additional products to be integrated and configured to minimize solution complexities and costs while maximizing value to Canada. What approach would PSPC like industry to follow to recommend solutions along with the effort to integrate and configure the solution to meet the full set of requirements?
- PSPC requires the Contractor to "design, develop, configure, test, implement, deploy and stabilize to a steady state, the Solution as illustrated in Figure 2" of ANNEX A – Statement of Work. Further PSPC indicates that "the identified suites that the Contractor must adhere to include" the products identified on page 31 of ANNEX A – Statement of Work. At the same time the RFP allows "software tools to be used by the Contractor that are not available from within the GC packaged inventory". Does the term "GC packaged inventory" refer to the products available on the GC SLSA or the products identified on page 31 of ANNEX A – Statement of Work?

Up to this point we have not received an answer to the above questions. Furthermore, the subsequent amendments expanded the need for products not included in Section 3, Technical Requirements, as follows:

Amendment 3, Change 32 removed Adxstudio Portal from Section 3, Technical Requirements while indicating: "The web portal will be used by External Users with defined roles and rights. The Contractor will provide and configure a technology that will reside on the GC network, interface seamlessly with the Dynamics CRM application, be scalable to meet future growth, use web services, and predominantly leverage configuration over customization."

The word "provide" in the paragraph above places the responsibility of procuring the portal technology on the Contractor. Which terms of this procurement define how the Contractor should provide the portal technology?

**Answer 204:**

For the purpose of certainty, Canada requires the Contractor to provision Professional Services and related Software as contemplated by the SACC Manual Supplemental General Conditions 4002 and 4007, referenced under item 7.3 of PART 7 – RESULTING CONTRACT CLAUSES.

Canada does not require Licensed Software, as contemplated by SACC Manual Supplemental General Conditions 4003 and 4004 during the initial delivery nor during the pre-production staging of the project. In the event that the Bidder sees a gap, opportunity or innovation that the Bidder considers materiel to their respective Bid, compliance or the resulting Solution, then the Bidder should refer to item 2.5 of PART 2 – BIDDER INSTRUCTIONS, and identify the suggested improvement according to the instructions therein, for Canada's consideration.

The term "GC packaged inventory" has been removed from the SOW, ANNEX A. Please refer to Change 113 in this Amendment.

**Question 205:**

With respect to Section 6: Testing Management, Subsection 1.2 Detailed Requirements, Category - Test Management (Test Type), TM09, please provide a definition of "path analysis testing" as used in this context.

**Answer 205:**

The definition of Path Analysis (or Basis or Branch Analysis) within this context is a method of identifying tests based on the paths (or flows) that can be taken through a system. There is evidentiary support that the majority of errors are detected on the first execution of a statement and path testing provides the best opportunities to expose those errors.

**Question 206:**

Within Amendment 3 and subsequent amendments, Canada introduced new requirements to the RFP (e.g. security controls in Amendment 3, software licenses in amendment 6). The amended requirements add cost and effort to the response, yet the financial envelope of $6-11 million remains unchanged. We are concerned that Canada has created an artificial 'floor' for the financial proposals, particularly given the additional requirements articulated in the amendments. In our experience, vendors will feel incented to de-scope or remove as many requirements as possible to reach the "floor" of $6-million, and then use the change control process to negotiate increases to their proposed price post award. In view of the amended requirements and in an effort to ensure compliance, we respectfully request that the financial envelope be adjusted to between $9-13 million, so that the Firm Lot Price Financial Bid Form 3 to Part 4 reads as follows:

"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 $9,000,000.00 and must not exceed $13,000,000.00. The prices must be in Canadian currency, Customs Duties are included and Applicable Taxes are extra."

**Answer 206:**

Please refer to the response provided to Question 194 in this Amendment 011.

**Question 207:**

The response to question 67 under Amendment No. 006 provides that the Contractor must procure and provide the license(s) to the GC as part of the contract. Per Section 1.2 Detailed Requirements SC.12 states that the Contractor must only allow authorized software, as documented by the Contractor and approved by PWGSC, to execute on the Solution. The requirement to hold the license on behalf of the Crown was not specified in the RFP previously, and is a significant change to the RFP. We note in addition that the financial tables in the RFP do not include pricing for software licensing.

We are concerned that the addition of new software requirements fundamentally changes the nature of the RFP and places a new requirement for Bidders to negotiate licenses to respond. To resolve this, Canada could choose to provide the software products referenced in Amendment 006 (Kingsway and Scribe) as Government Furnished Equipment ("GFE"). Accordingly, we respectfully request that these software products (specifically Kingsway and Scribe) be provided as GFE, or that Bidders be allowed to meet the Exact Transfer Load ("ETL") requirements using SQL Server Integration Services ("SSIS") with APIs.

**Answer 207:**

APP-DM.04 has been updated to provide clarity on the Contractor's role in regards to data migration activities. With respect to software products, please refer to Question 204 in this Amendment.

**Question 208:**

The RFP and proposed Resulting Contract Clauses do not allow for vendors to provide software licenses under the Terms and Conditions of this eventual contract. Further, Amendment 6, Answer 67 directly contradicts this statement in that "The contractor must procure and provide the license(s) to the GC as part of the contract. Further, the pricing table, current described budget, and financial evaluation scheme do not allow for contractors to include the price of any provided software. Would the Crown provide clear expectations and instructions as to how a contractor should propose and provide software licenses given the restrictions above?

**Answer 208:**

Please refer to Question 204 in this Amendment.

**Question 209:**

Amendment 8 Change 86 introduces R10.C which has a table of SOW requirements to be declared as met "Out of the Box (OB)" or "Requires Configuration (RC)". ISST SOW Glossary defines Configurable as: "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". As most OB capabilities will require some level of configuration (as defined above) please consider replacing "Requires Configuration" with "Requires Customization". This better reflects the intent of the rated requirement, namely that OB (which typically requires configuration) does not require modification or development to meet requirement. If development or modification is required to meet the requirement it would be assessed as "Requires Customization (RC)".

**Answer 209:**

Please see the response to Question 210 in this Amendment.

**Question 210:**

Amendment 8 Change 83 introduced mandatory requirement M3 Corporate Reference Projects: COTS Solution which requires demonstration that the proposed technology has the ability to meet the requirements referenced in Section 2, 3 and 4 in Annex 1 SOW. Section 2 specifies three sets of functionality that do not directly relate to the COTS Web Portal: Business Process Re-engineering (BR.xx series), Service Processing Application (APP-xx series for automation, operations support, user experience, information management, communications, paperless, interconnectivity, reporting and analytics) and Data Migration (APP-DM.xx). The actual COTS Web Portal functional requirements are at 2.2.2 Web Portal (WP.xx series) and the technical requirements are at Section 3 Tech.48 through Tech.55.

In order to clarify scope of bidder's response for the proposed COTS Web Portal, can PSPC confirm that the M3 Corporate Reference Projects: COTS Solution should demonstrate ability to meet the COTS Web Portal requirements specified in Section 2 - Business Requirements, para 2.2.2 Web Portal (WP.xx) and Section 3 - Technical Requirements, para 1.2 COTS Web Portal requirements Tech.48 through Tech.55? This refinement will focus the bidder responses on the actual COTS Web Portal requirements and simplify GC assessment.

**Answer 210:**

Canada has replaced the term "COTS Web Portal" with "Vertical Public Facing Web Front-End Service" within ANNEX A and the Technical Evaluation.

As a result M3 and R10 have been removed and the Technical Evaluation has under gone some revisions.

Please refer to Change 127 in this Amendment.

**Question 211:**

Section R1 c) of the RFP states: "For each project activity and milestone, the associated deliverables including the critical path used to achieve said deliverables;"

Will the Crown accept the Microsoft Project schedule, delivered for requirement R1 d), containing the sequenced list of tasks that drive each of the project activities and milestones as demonstration of the critical path to deliver each of the said deliverables and milestones? If the Crown prefers a different format for this information, please provide an example detailing how this information is to be presented.

**Answer 211:**

Canada will accept the submission of the schedule requested in R1 (d) in a Microsoft Project schedule format.

**Question 212:**

In R1, the Crown indicates that "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**".

Further, the Crown indicates that "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**".

Would the Crown please confirm that the evaluation of the Vendor's response will be based on ANNEX A, Section 2 to 7?

**Answer 212:**

Note that Canada identifies that the Preliminary Project Plan should reflect a strategy that will successfully implement requirements listed from 2 to 7, while supporting the outcomes outlined in Section 1 and 7. These outcomes include, but are not limited to Section 1, 1.1.2.1 and 1.1.2.2 and Section 7, 2.1, the paragraph stating "Effective Change management is intended to:"

**Question 213:**

In Amendment 8, Change 83, the Crown added a new M3 requirement as follows:
Corporate Reference Projects: COTS Solution
The Statement of Work identifies the requirements for the COTS web portal technology. The bidder must provide a full description of the COTS web portal technology that will be installed on GC premises including:

a) Product and version;
b) Server requirements;
c) Database requirements; and
d) Integrability with MS Dynamics (on-premises) 2015 or higher.

The response must also demonstrate that the proposed technology has the ability to meet the requirements referenced in Sections 2, 3 and 4 in Annex 1.

The title of this Requirement "Corporate Reference Projects" implies that we need to respond with a project reference, but the requirement itself is asking only for a full description of the proposed COTS Portal Solution.

Would the Crown please confirm that only the description of the proposed COTS Solution is required in response to M3, and that a Project Reference is not required in response to M3?

**Answer 213:**

Evaluation Criteria M3 has been removed from the Technical Evaluation, please see the response to Question 210 in this Amendment for further information.

**Question 214:**

In Amendment 8, Change 83, the Crown added a new M4 requirement as follows:

**Customer References**
For each Reference Project provided in response to M1, M2 and M3, the Bidder must complete Form 2 to Part 4. The client contact may be contacted to validate the information provided in the Bidder's response, in accordance with Part 4.2.4, Reference Checks.

As M3 does not require a Project Reference, would the Crown modify M4 to exclude M3?

**Answer 214:**

M4 has been updated with the removal of evaluation criteria M3. Please see the response to Question 210 in this Amendment for additional information.

**Question 215:**

In Form 3 to Part 4 the Crown requested the Total Firm Lot Price must not be less than $6,000,000.00. In the initial issue of the RFP the Crown anticipated that all software required for implementing the solution would be provided by the Crown. However, in Amendment 8 the Crown requested the Bidder to provide the portal technology software. Given that Bidders will incur this extra cost in delivering the solution we request the Crown change the Total Firm Lot Price to be no less than $7,000,000.00.
Further, it is standard practice that Canada abide by software licensing terms issued by the publisher as it will be the end user. Can Canada indicate the method by which it will accept these terms? Failure to do so would impede vendors from including additional software as licensing terms cannot be accepted by the vendor on behalf of Canada nor can these terms, in whole or part, be assigned to Canada after the fact.

**Answer 215:**

Please refer to the responses provided to Questions 194 and 204 in this Amendment 011.

**Question 216:**

The volumetric requirements for M1 (number of user accounts, number of transactions, and number of diverse transactions) are prohibiting us to use some of our corporate reference projects that have several suitable similarities and many relevant commonalities with the ISST project requirements for Business Process Re-Engineering and Change Management solutions and services. Those corporate reference projects are clearly compliant to all the other M1 requirements and evaluation criteria and are fully demonstrating our capabilities and capacity to deliver BPR and CM services for projects like ISST. We, therefore, request that M1 be modified to request that 2 instead of the 3 corporate reference projects required for M1 meet the prescribed volumetric requirements, which will still demonstrate the proper extent and level of past performance required for the ISST.

**Answer 216:**

Canada has amended M1 and M2 to require that 2 projects meet the volumetrics instead of 3. Bidders will still be required to submit three projects in total. Please refer to Change 127 and the response to Question 172 in this Amendment.

**Question 217:**

We are going through a review, validation, and revision of our effort estimation for the delivery of the ISST project against the RFP Annex A SOW requirements. Would PSPC share with us their rationale behind the prescribed $6M to $11M price range for the delivery of the fixed price 29-month project, so that we can better align our scoping and sizing of the project accordingly?

**Answer 217:**

Please note the lower limit for the Total Firm Lot Price has been raised to $8M to reflect the changes in high integrity controls. Please see the response to Question 194 in this Amendment 011. It is the responsibility of the Bidder to propose a response that is compliant with the financial requirements, while scoping the project to the requirements listed in the SOW and rationalizing their costs on factors such as level of effort, number of resources, etc. Canada has done the same activity it is asking bidders to complete, which generated the $8M to $11M envelope.

**Question 218:**

Could PSPC, please, confirm that the four 6-month options to the initial contract term are not related to the Firm Lot Price table but only to the As-and-When Requested Work Price Table for the Financial Proposal?

**Answer 218:**

Canada confirms that the Firm Lot Price table does not relate to the four 6-month option periods, nor other "as-and-when-requested" work. The Contractor must deliver the requirements related to the Firm Lot Price within the original Contract Period of 29 months.

**Question 219:**

In reference to the Industrial Security Systems Transformation Request for Proposal (EP243-170549/B) - Amendment 8, Question and Answer 110, could the Crown please confirm that no link will be provided to enable remote testing of non-production data?

**Answer 219:**

There is no intention to establish a remote link to the Dynamics environment. Remote access for testing the Vertical Public Facing Web Front-End Services is expected to be a normal requirement.

**Question 220:**

Per Amendment 3, change 21, it stipulated "7.4.7. The Contractor must complete and submit a Foreign Ownership, Control and Influence (FOCI) Questionnaire and associated documentation identified in the FOCI Guidelines for Organizations prior to contract award to identify whether a third party individual, firm or government can gain unauthorized access to INFOSEC information/assets. Public Works and Government Services Canada (PWGSC) will determine if the company is "Not Under FOCI" or "Under FOCI". When an organization is determined to be Under FOCI, PWGSC will ascertain if mitigation measures exist or must be put in place by the company so it can be deemed "Not Under FOCI through Mitigation".

Can the Crown please confirm that this questionnaire is not required to be submitted by proposers with their bid and if not, can PWGSC be able to provide the questionnaire to be completed in advance of bid closing so that we may be compliant with this requirement prior to contract award.

**Answer 220:**

Canada confirms that the FOCI questionnaire is not required to be submitted with the bid at bid close. Please note that the response to Question 160 in Amendment 009 contained an error – the questionnaire and related documentation must be submitted upon request, prior to contract award. Please refer to item 7.4.7 of Part 7 Resulting Contract Clauses for clarity.

**Question 221:**

In amendment 8, Canada added two new requirements related to portal technology, requirements M3 and R10. The requirements in R10 are extensive in that they rate 6+ implementation examples with the proposed portal, and also rate out of the box versus configuration requirements. Since Canada has narrowed the requirement to only portal experience with the proposed portal solution, this could require Bidders to identify up to 6 new credentials before bid closing, which is onerous and most likely not Canada's Intention.

Portal technology/experience is already a component of M1 and M2. We suggest that R10 be revised to a maximum of 2 examples with the proposed solution. We believe this is a reasonable demonstration of experience, and fair given the time available before the bid submission date.

For illustrative purposes, our proposed revision would revise the R10 requirement as follows:

*"At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria:*
*INSERT*
***R10***
***COTS Web Portal***
*Based upon the COTS Web Portal technology proposed in response to M3, The Bidder should indicate whether the proposed portal technology has been successfully implemented in other solutions, whether it has a licensing model and if it has out of the box functionality to meet requirements in the SOW, or requires functionality built in and would require additional configuration.*
*A. The Bidder should demonstrate that they have successfully implemented the portal technology in other Reference Projects. Bidders are requested to complete Form 2 to Part 4 for all Reference Projects provided in response to R10 for up to 2 reference projects should be with the proposed portal solution. The client contact may be contacted to validate the information provided in the Bidder's response, in accordance with Part 4.2.4, Reference Checks.*
*B. The Bidder should describe the proposed licensing model including renewal, support and software assurance. The licensing model should be submitted in order to obtain points for this criteria.*
*C. The Bidder should complete the following table by placing an X in the appropriate column, to indicate whether the requirement will be met by the Web Portal Technology proposed in response to M3 out of the box (OB), or if it*
*will require configuration (RC):…"*

**Answer 221:**

Evaluation criteria M3 and R10 have been removed from the Technical Evaluation, please refer to the response to Question 210 in this Amendment for additional information.

**Question 222:**

Given the restrictions from Amendment 008, answer 110 ("In addition no electronic link will be provided between the GC and Contractors IT systems") should vendors assume that in order to access a properly configured GC IBM Pure Data warehouse instance, for non-production uses, that vendor resources must go on-site to gain access (this question is asked so that all vendors are evaluated equally given the new restriction)?

**Answer 222:**

The Crown confirms that all project work that requires an individual to have direct access to GC protected information and assets are required to be on-site. As indicated to access the GC IBM Pure Data warehouse instance will require the Contractor to be located on-site.

For additional information, please see response to Question 219 in this Amendment.

**Question 223:**

Given that :

a) many of our questions still remain unanswered;

b) the due date for questions was September 5;

c) industry will still be left with too little time to appropriately amend proposals in response to changes by the Crown specified in any new amendments, and will have no time remaining to ask for clarifications to those changes;

We respectfully request that the Crown extend the RFP bid close date to September 30, 2017.

**Answer 223:**

The date of bid closing has been extended to October 2, 2017.

**ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME**

# 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 appropriate 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 Cyber Authentication Services technology to access the ISST Solution's Vertical Public Facing Web Front-End Service in order to submit service requests to the ISST Solution's Service Processing Application. Please refer to http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262 for more information on the GC Cyber Authentication Service. 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 to CSP and CGP inspectors and investigators.

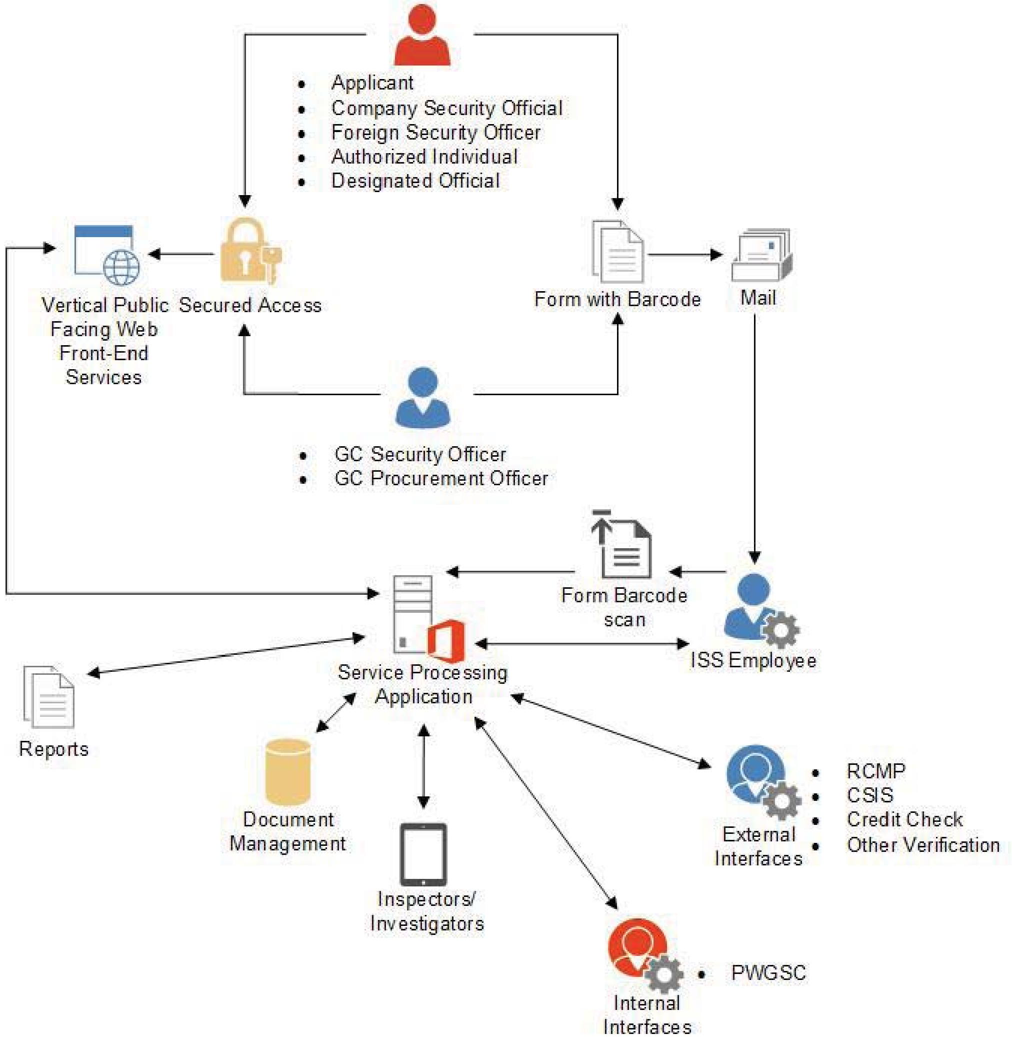


**Figure 1:** ISST Solution high level interaction map.

## 3.1 VOLUMETRIC DATA

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

### 3.1.1 User Accounts

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

External User Accounts: Current total of 183,905 user accounts which breaks down as follows:

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

*Note: Currently CGP does not have any External User Accounts. However, it is estimated that the Solution will facilitate access to approximately 22,000 CGP External User accounts.

### 3.1.2 Activity Specific Volumes

Represented below are the different transactions within the ISS business with an indication of annual and daily 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:<br>(a) Elaborating on objectives for business process re-engineering as it relates to the ISST Solution;<br>(b) Strategic purpose of business process re-engineering as part of the ISST Solution;<br>(c) Expand on how the business process re-engineering gap analysis will be conducted; and<br>(d) Elaborate on how the constraints and impacts will be addressed as a result of the business processing re-engineering; and<br>(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 after business process re-engineering and Solution design to identify areas (e.g. business processes and users) 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. |
| | BR.19 | Prepare a Preliminary Business Process Re-engineering Strategy which includes, but is not limited to:<br>(a) An understanding of the current ISS business processes and the need for security practices within the various business operations;<br>(b) A plan to conduct a business process gap analysis;<br>(c) An understanding of constraints and impacts;<br>(d) Four examples of opportunities to improve process efficiency and effectiveness and proposed implementation approaches;<br>(e) An understanding of risks and options for risk resolution or mitigation; and<br>(f) Scheduling of business process re-engineering activities. |
| | BR.20 | Prepare a Business Process Re-engineering Strategy after the Preliminary Business Process Re-engineering Strategy has been evaluated by Canada and deemed that the strategy meets the benefits and requirements identified above. |

## 2.1 REQUIREMENT OVERVIEW – FUNCTIONAL REQUIREMENTS

The Solution is a business application composed of two major components: a Service Processing Application and a Vertical Public Facing Web Front-End Service.

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 reporting on ISS business activities and trends through available reports; and
(l) A Solution that implements the core services rendered by the ISS;

The Vertical Public Facing Web Front-End Service 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 Vertical Public Facing Web Front-End Service 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):<br>(a) For service request satisfying all mandatory criteria (e.g. security partner verifications);<br>(b) Notification sent to External User indicating that their service request was approved;<br>(c) Generation of appropriate approval certificate with corresponding signatures and validation dates of the request; and<br>(d) Availability of appropriate approval certificate to the External User for download/printing from the Vertical Public Facing Web Front-End Service. |
| | APP-AU.03 | Automatic management of user accounts:<br>(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*;<br>(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;<br>(c) Automatically disables accounts belonging to organizations that are no longer registered (or terminated) with the ISS; and<br>(d) Automatically deletes all disabled accounts after a predefined period of time. |
| | APP-AU.04 | Automatic population of the External User's vertical public facing web front-end service calendar feature with pre-defined events relating to service requests submitted to ISS (e.g. correspondence due dates, organizational registration renewals, etc.). |
| | APP-OPS.01 | Enforces a Role Based Access Control over all defined users and objects. |

| Category | SOW NUM | Requirement |
|---|---|---|
| Operations Support | 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 vertical public facing web front-end service and internal processing application. For example, to be able to modify the solution parameter defining the standard number of days to complete 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 vertical public facing web front-end service. |
| | 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). |
| | 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). |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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 vertical public facing web front-end service. 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 (application only, no data) 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 Users can access from the Solution Vertical Public Facing Web Front-End Service to gain access to the Sandbox/Training environment. See business requirement WP-UE.22. |
| | 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:<br>(a) Development;<br>(b) Testing;<br>(c) User Acceptance Testing;<br>(d) Staging; and<br>(e) Production. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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-OPS.25 | Provides unique identifiers to system objects such as cases and companies that can be viewed and referenced by internal and external clients. |
| 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.<br>(a) This selection must include English and French interfaces; and<br>(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. |
| | 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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. |
| | 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 ISS' 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 from within the Solution. |
| | 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. |
| | 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | APP-IM.27 | Enables Internal Users to retrieve archived records from a case file for a specified retention time as determined by the business. Available archived files are to be accessed from within the Solution. |
| | 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 email notifications resulting from predefined events such as decisions 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 vertical public facing web front-end service 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 attachment of scanned documents to case files. |
| | 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 vertical public facing web front-end service 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). |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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). |
| 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.<br>The SABA learning software serves as the Industrial Security Sector's standard platform to deliver extended learning courses for the Contract Security Program and the Controlled Goods Program. The platform will host different training types (i.e. e-classroom, PowerPoint presentations) in a variety of formats, in both official languages. SABA will also maintain certifications, including automated exam administration. Reports and analytics for learning activities will also be generated through SABA. The solution must have the ability to ingest updates from SABA pertaining to completed training in order for service requests to be processed. |
| | 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 vertical public facing web front-end service into the processing application. It must also be 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. |
| | APP-ICN.06 | Interfaces with the RCMP to allow the RCMP to send updated security information on an as and when required basis. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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. |
| 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. |
| | 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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 Solution's suite of standard reports externally (vertical public facing web front-end service) 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 vertical public facing web front-end service. |
| | 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:<br>(a) Personnel Security Screening Services;<br>(b) Organization Registration Services;<br>(c) Inspections and Investigations Services;<br>(d) Contract Security Services (including Visit and Document Control requests);<br>(e) Controlled Good Services; and<br>(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 Vertical Public Facing Web Front-End Service

The Contractor must deliver a Vertical Public Facing Web Front-End Service that provides the following functionalities, but is not limited to:

| Category | SOW NUM | Requirement |
|---|---|---|
| | WP-SH.01 | Enables secure access for External Users at logon. |

| Category | SOW NUM | Requirement |
|---|---|---|
| Service Hub | WP-SH.02 | Uses approved government methods for user identification and authentication (e.g. Secured Access, 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 Vertical Public Facing Web Front-End Service and the Services Processing Application. |
| | WP-SH.06 | Enables External Users to submit and manage service requests, including but not limited to:<br>(a) Complete service request forms;<br>(b) Save and revisit incomplete forms; and<br>(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:<br>(a) View completed milestones/activities;<br>(b) View pending milestones/activities; and<br>(c) View estimated completion timeline. |
| | 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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 email 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. 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 vertical public facing web front-end service at any time using any device. This includes electronic signatures. |
| | WP-UE.06 | Enables External Users to access the vertical public facing web front-end service from tablets equipped with Internet browser, without any loss of vertical public facing web front-end service functionalities. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | WP-UE.07 | DELETED |
| | WP-UE.08 | Enables External Users to receive system wide notifications such as services interruptions, etc. |
| | WP-UE.09 | Enables External Users to receive standardized email messages pertaining to service request updates. |
| | WP-UE.10 | External Users can print completed forms containing all inputted information for their records or for submission to the ISS for processing, using the Vertical Public Facing Web Front-End Services. |
| | WP-UE.11 | Provides access to downloadable fillable forms that must contain the same data fields as their online counterparts for user completion. |
| | 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-nPPL.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 vertical public facing web front-end service 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. |
| | 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 vertical public facing web front-end service 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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.<br>(a) This selection must include English and French interfaces; and<br>(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 | DELETED. |
| | 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-as 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. |
| | APP-DM.02 | Develop a Data Migration Plan which includes:<br>(a) A detailed description of all activities required to complete Data Migration from the legacy systems to the Solution, including:<br>i. Data analysis;<br>ii. Migration tools development/configuration;<br>iii. Migration testing;<br>iv. Data migration validation; and<br>v. Data migration documentation.<br>(b) A proposed schedule for completion of all described Data Migration activities. The proposed schedule must respect the timelines identified within the Project Schedule.<br>(c) An estimate of number and categories of resources required to complete each migration activity and a breakdown of associated costs. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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 | Support the GC with guidance and documentation in the migration of sample data and data validation. Assess integrity of data and impacts of migration. 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 a solution based on the requirements, the High Level ISST Solution Conceptual Architecture and using the technologies listed in this statement of work. The Solution must be user friendly, reliable, maintainable, scalable, interoperable, extendable to accommodate the modification, adjustment, or addition of business process workflows, system automated functions, and compliant with GC IT/IM policies, guidelines and environment.

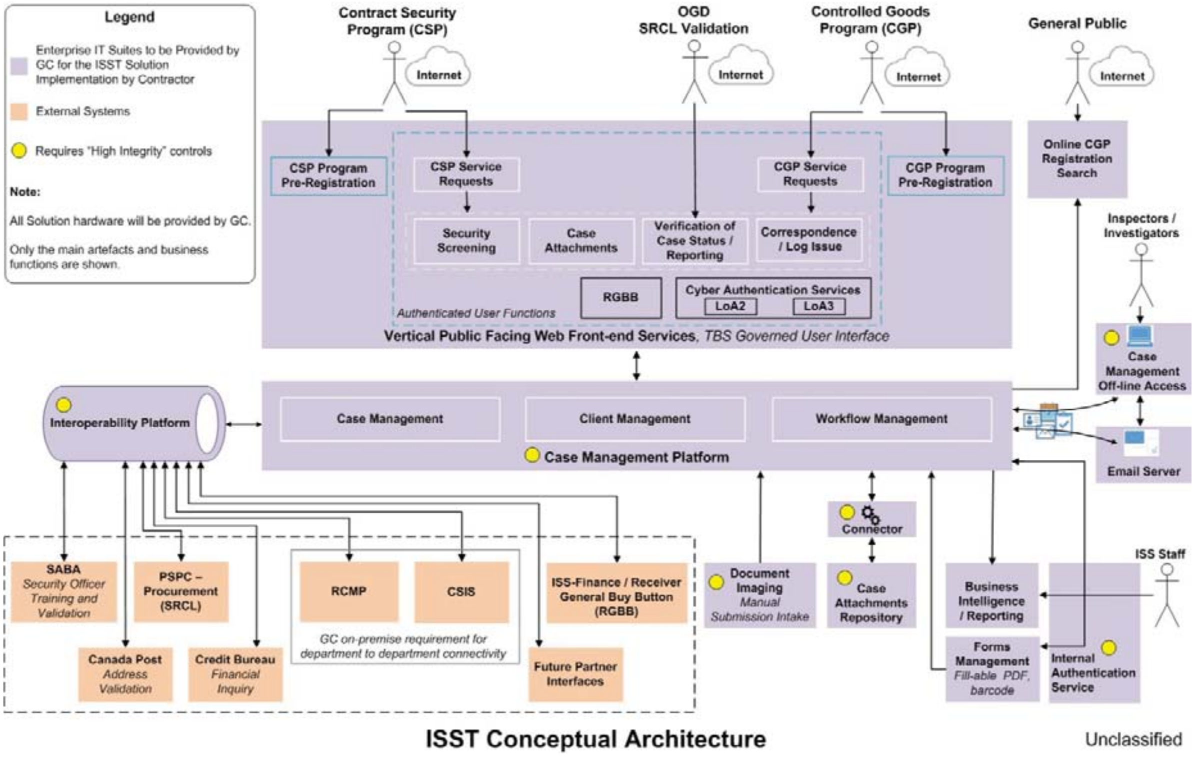

Legend
Enterprise IT Suites to be Provided by GC for the ISST Solution Implementation by Contractor
External Systems
Requires "High Integrity" controls
Note:
All Solution hardware will be provided by GC.
Only the main artefacts and business functions are shown.
Contract Security Program (CSP)
Internet
OGD SRCL Validation
Internet
Controlled Goods Program (CGP)
Internet
General Public
Internet
CSP Program Pre-Registration
CSP Service Requests
CGP Service Requests
CGP Program Pre-Registration
Online CGP Registration Search
Security Screening
Case Attachments
Verification of Case Status / Reporting
Correspondence / Log Issue
RGBB
Cyber Authentication Services
LoA2
LoA3
Authenticated User Functions
Vertical Public Facing Web Front-end Services, TBS Governed User Interface
Inspectors / Investigators
Case Management Off-line Access
Interoperability Platform
Case Management
Client Management
Workflow Management
Case Management Platform
Email Server
Connector
ISS Staff
SABA Security Officer Training and Validation
PSPC – Procurement (SRCL)
RCMP
CSIS
GC on-premise requirement for department to department connectivity
ISS-Finance / Receiver General Buy Button (RGBB)
Document Imaging Manual Submission Intake
Case Attachments Repository
Business Intelligence / Reporting
Canada Post Address Validation
Credit Bureau Financial Inquiry
Future Partner Interfaces
Forms Management Fill-able PDF, barcode
Internal Authentication Service
ISST Conceptual Architecture
Unclassified

**Figure 2:** High Level ISST Solution Conceptual Architecture

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.

External Users, such as Contract Security and Controlled Goods Program applicants, will access the functionality required for their business processes via the Vertical Public Facing Web Front-end Services. These users will gain access to the environment after being authenticated at the appropriate level of assurance required by the application using the cyber authentication services and based on defined roles and rights. There will be **no** direct access to the MS Dynamics CRM core platform by External Users. The Vertical Public Facing Web Front-end Services platform will host web enabled forms for the requisition of and receipt of services. The configuration of Vertical Public Facing Web Front-end Services enabling business intake processes interfaces must meet GC requirements (WCAG) for web standards.

The Contractor will configure technology that will reside on the GC network, interface with the Dynamics CRM Case Management Platform, be scalable to meet future growth, use web services, and predominantly leverage configuration over customization.

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.

The Solution must leverage PWGSC identified technology in the descriptive list below. These technologies are Enterprise IT Target Suites that are driven by the Chief Information Officer Branches (CIOB) of TBS or PWGSC, in order to reduce and streamline the application footprint for GC and PWGSC applications. Wherever possible, the Contractor must meet the requirements of the Solution, including any new requirements driven by business process re-engineering through leveraging these technologies to build a unified Solution.

The identified Enterprise IT Target Suites that the Contractor must adhere to include, but are not limited to:

**(a) Dynamics CRM (On premise) 2015 (or higher) (Enterprise IT Target Suite)**
**Case Management Technology** - The Vertical Public Facing Web Front-end Services for business intake 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.

**(b) Microsoft Exchange Server, Outlook Client (Enterprise IT Target Suite) and MS Dynamics CRM for Outlook GC e-mail** – This technology will be used to support e-mail and off-line Case Management capabilities for internal users such as field inspectors.

**(c) SAP Business Objects (Enterprise IT Target Suite)**
**Business Intelligence Reporting** - SAP Business Objects BI 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 BI connected to a PureData warehouse. Reporting functionality must be available to both Internal and External users based on the users' application profiles.

**(d) Oracle Service Bus (Enterprise IT Target Suite) Information Sharing Technology** - GC Interoperability Platform (GCIP – based on Oracle Service Bus (technology). Information sharing between ISS and partner organizations should be automated and managed in accordance with GCIP capabilities and the underlying Oracle Service Bus technology.

**(e) Imaging/Scanning System -** This system is in place and uses IBM DataCap technology. The ISST Solution will need to exchange information with this system.

(f) **Documents and Records Management System -** The Solution is expected to require the storage, management and retrieval of data largely grouped into two categories: (1) Database or Data Management System - processing-intensive, higher transaction structured data typically associated with in-process requests and with company and personnel data, and (2) Document and Records Management System – unstructured data typically associated with attachments that should not be altered but must be retained for document & records management and evidentiary purposes (e.g. passports, birth certificates etc.), representing low transaction, infrequent retrieval rate processing.

i) **Database or Data Management System -** The Contractor must leverage existing products already licensed and in use by PSPC, to satisfy the requirements for non-sensitive, sensitive, and intensive information/data processing purposes. The solution should use the GC standards of SQL Server/Oracle for any database applications.

ii) **Documents and Records Management System -** The current GC standard for document and records management is OpenText Content Server, which should be leveraged for unstructured data long-term storage. This would be the default for items which are not required for dynamic processing, and includes (but is not limited to) static attachments and manually submitted forms that are digitized for document and records management purposes.

The Contractor must provide IM/IT technical expertise in the areas of application development particularly configuration and integration of various technology platforms as outlined in this statement of work; 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, 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 | Enables and implements 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. |

| SOW NUM | Requirement |
|---|---|
| Tech.05 | Enables and implements automatic termination of an open web session after a period of inactivity as determined by GC. |
| Tech.06 | Enables and implements 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:<br>(a) PDF (Adobe PDF);<br>(b) DOC, DOCX (MS word 2013 and above); and<br>(c) XLS, XLSX (MS Excel 2013 and above). |
| Tech.07 | Implements the solution for supporting 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 | Implements the solution 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). |
| 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 | Implements 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 | Implements 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 Vertical Public Facing Web Front-end Services to enable business intake processes such as creating web enabled forms to gather and exchange information, and that 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. |

| SOW NUM | Requirement |
|---|---|
| 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 the applicable "Protected B, High Integrity, Medium Availability" (PB/H/M) security profile requirements for the platforms as identified on the ISST Conceptual Architecture diagram. |
| Tech.18 | Ensures conformance with the GC Web Standards (https://recherche-search.gc.ca/rGs/s_r?cdn=canada&st=s&num=10&langs=en&st1rt=1&s5bm3ts21rch=x&q=web+standards&_charset_=utf-8&wb-srch-sub=) and Web Accessibility (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601) requirements for the Vertical Public Facing Web Front-end Services enabled business intake processes. |
| 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. |
| 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:<br>(a) Near Real-Time or batch;<br>(b) Web services / APIs;<br>(c) XML and/or Flat file;<br>(d) Export and import of data and content; and<br>(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. |

| SOW NUM | Requirement |
|---|---|
| Tech.26 | Leverages and supports GC and IT industry best practices and standards that have been adopted widely for building and maintaining a high-performing IT system to:<br>(a) Provide easy-to-use Web applications;<br>(b) Ensure and maximize the maintainability of the Solution;<br>(c) Ensure and achieve high level reliability;<br>(d) Ensure scalability and sustainability; and<br>(e) Deliver acceptable system performance. |
| Tech.27 | Supports GC's strategic plans for application interoperability, including, at a minimum by:<br>(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<br>(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.<br>The following is a list of types of expected technologies that must be supported:<br>(a) SAML 2.0<br>(b) JSON<br>(c) Kerberos<br>(d) X.509<br>(e) LDAP<br>(f) RBAC<br>(g) OAuth<br>(h) SOAP<br>(i) REST<br>(j) oData |
| Tech.29 | Supports, uses and/or develops structured and modular external interfaces which allow information exchange between the Solution and other systems through a secure communications infrastructure.<br>These interfaces include, at a minimum:<br>(a) An intranet or extranet for the business processes described in "Section 2: Business Requirements";<br>(b) Web services – third party data feeds;<br>(c) Commercially available third party security components such as Public Key Infrastructure (PKI) products; and<br>(d) GC or NGO systems containing supporting information needed to process transactions. |

| SOW NUM | Requirement |
|---|---|
| Tech.30 | Interoperates with other systems and platforms, as indicated in Figure 2, using as a minimum the following:<br>(a) APIs;<br>(b) Export and import of data and content; and<br>(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 ISST Logical and Physical architecture blueprints (using GC templates) based on the ISST Conceptual architecture blueprint. These blueprints are subject to GC approval. |
| 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. |
| Tech.36 | Design and create a data architecture which:<br>(a) Includes all appropriate data models, specifically, conceptual, logical, and physical;<br>(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;<br>(c) Includes data dictionaries;<br>(d) Will operate within the ISS solution environment;<br>(e) Supports all ISS business processes; and<br>(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. |

| SOW NUM | Requirement |
|---|---|
| Tech.38 | Develop detailed interface documentation, including but not limited to:<br>(a) Concept of Operations;<br>(b) Systems Overview;<br>(c) Interface Overview (for every Interface in, to and from the application);<br>(d) Functional Allocation;<br>(e) Data Transfer;<br>(f) Transactions;<br>(g) Security and Integrity;<br>(h) Detailed Interface Requirements;<br>(i) Interface Processing Time Requirements;<br>(j) Message (or File) Requirements;<br>(k) Communication Methods;<br>(l) Security Requirements;<br>(m) Qualifications Methods;<br>(n) Approvals; and<br>(o) Record of Changes. |
| Tech.39 | Provide a Solution that allows for the management of forms via configuration in Dynamics (or another means) without the need of a developer. |
| Tech.40 | Design the solution to ensure that “digital signatures” are used for both, internal user and internal service initiated processes where required. |
| Tech.41 | Identify and describe, within their physical architecture design, the security controls to be implemented by the Contractor, and the GC. |
| Tech.42 | Define the contents for and configure the solution to produce system generated audit files to include information to facilitate integrity violations determination. |
| Tech.43 | Configure the solution to enforce user account restrictions (e.g. time of day, day, week, etc.) |
| Tech.44 | Create a process that will store previous configurations of the solution to support version rollback for a period to be defined by the GC. |
| Tech.45 | Configure the solution to prevent unauthorized and unintended information transfer via shared system resources. |
| Tech.46 | Configure the solution to respond automatically when integrity violations occur. |
| Tech.47 | Configure the solution that meets the requirements of the current solicitation. |
| Tech.47.A | Provide Detailed Design Specifications |
| Tech.47.B | Provide a Relationship Management Approach, including the following elements:<br>(a) Overall approach to Government of Canada and Contractor relationship management; |

| | |
|---|---|
| | (b) Communications between the Government of Canada and the Contractor in respect to a proposed governance model and team structure as detailed in R1. A.;<br>(c) Issue management and resolution;<br>(d) Joint planning and managing of changes to project scope and schedule |

The Contractor must utilize a Vertical Public Facing Web Front-End Service for business intake technology that:

| | |
|---|---|
| Tech.48 | Installs and operates on a Windows 2012 server platform, and Internet Information Services (IIS) web server. |
| Tech.49 | Leverages predominantly, configuration vs. customization. |
| Tech.50 | Resides on the GC network and is scalable. |
| Tech.51 | Is configured to allow Government of Canada Credential Federation (GCCF) Credential integration. |
| Tech.52 | Interfaces/integrates with MS Dynamics CRM (2015 or later) using web services and/or other approved and supported methods by the underlying technology platforms for its integration with Dynamics CRM Case Management Platform. |
| Tech.53 | Supports content creation and publishing in Canada's official languages – English and French. |
| Tech.54 | Supports wireless and mobile devices. |
| Tech.55 | Supports encryption. |

# 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 (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.

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.06 | Ensures that Microsoft Dynamics CRM is accessible through a VPN. |
| SecureInt.07 | Uses digital signatures for Internal Users related processes where required. |

### 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 Vertical Public Facing Web Front-End Service. |
| 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.

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.

| SA&A Gate | Requirement |
|---|---|
| SAAG.01 | The Contractor must complete:<br>(a) Security High Level Solution Design (SHLSD); and<br>(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:<br>(a) Security Detailed Solution Design (SDSD);<br>(b) Updated Security Requirements Traceability Matrix (SRTM);<br>(c) Change Management Procedures;<br>(d) Operational Security Procedures; and<br>(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:<br>(a) Security Installation Verification Plan;<br>(b) Security Installation Verification Report;<br>(c) Security Integration Test Plan;<br>(d) Security Integration Test Report;<br>(e) Updated SRTM with Security Integration Test Report mapping to security requirements;<br>(f) Vulnerability Assessment Plan; and |

| SA&A Gate | Requirement |
|---|---|
| | (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. 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 table below details the security requirements derived from the ITSG-33 controls that are the responsibility of the Contractor. The requirements listed here exclude those controls that are expected to be met by PWGSC as an organization through existing technology implementations. The Contractor will be responsible to incorporate all security controls, including those met by PWGSC, SSC and the Contractor, in the Security Requirements Traceability Matrix.

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.00.A | The Contractor must prepare a User Access Control and User Management Plan. |
| | SC.01 | The Solution must:<br>(a) Enforce role-based access controls for all individual users;<br>(b) Organize users into roles designed using the principles of “least privilege” and “need-to-know”;<br>(c) Automatically disable inactive or unused accounts after a period of time determined by the business;<br>(d) Create audit records regarding the creation, modification, removal, enabling, and disabling of accounts;<br>(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;<br>(f) Retain the session lock until the user re-establishes access using established identification and authentication procedures;<br>(g) Attribute the creation of any account to a single, specific individual;<br>(h) Require the use of non-privileged accounts or roles, when accessing non-security functions;<br>(i) Limit the number of unsuccessful login attempts before locking the account;<br>(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;<br>(k) Notify the user of any changes to their account roles and permissions since the last successful login;<br>(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<br>(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:<br>(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;<br>(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);<br>(c) Generate audit records of security events in a format suitable for submission to a Security Information and Event Management (SIEM) system; and<br>(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:<br>(a) Protect audit information from unauthorized access, modification, and deletion; and<br>(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:<br>(a) uniquely identify and authenticate organizational users; and<br>(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:<br>(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;<br>(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<br>(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:<br>(a) Fully document any connections between IT systems including data descriptions, data flows, security and access requirements and mechanisms, performance, and reliability expectations; and<br>(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:<br>(a) Analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice;<br>(b) Informing PWGSC of potential security impacts prior to change implementation, and<br>(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 PB/H/M. |
| Information Security Architecture | SC.16 | The Contractor must document the information security architecture for the Solution that:<br>(a) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of information;<br>(b) Describes how the information security architecture is integrated into and supports the enterprise architecture; and<br>(c) Describes any information security assumptions about and dependencies on, external services. |

| Category | SOW NUM | Requirement |
|---|---|---|
|  | SC.17 | The Contractor must provide a Security High Level Solution Design (SHLSD) that includes, at a minimum:<br>(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;<br>(b) The architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer);<br>(c) A description of the network zone perimeter defences;<br>(d) A description of the use of virtualization technologies, where applicable;<br>(e) Descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;<br>(f) Descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements;<br>(g) A description of the approach for:<br>i. Remote management;<br>ii. Access control;<br>iii. Security management and audit;<br>iv. Configuration management; and<br>v. Patch management.<br>(h) Justification for key design decisions. |
|  | SC.18 | The Contractor must provide a Security Detailed Solution Design (SDSD) that includes, at a minimum:<br>(a) A detailed component diagram (this must be a refinement of the high-level component diagram);<br>(b) Descriptions of the allocation of technical security mechanisms to detailed service design elements;<br>(c) Descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements; and<br>(d) Justification for key design decisions. |

| Category | SOW NUM | Requirement |
|---|---|---|
| Boundary Protection | SC.19 | The Solution must:<br>(a) Be implemented in such a way as to be resistant to denial of service attacks in order to meet ISS availability targets;<br>(b) Monitor and control communications at external boundaries of the Solution (internet facing and GC facing);<br>(c) Be configured to deny communication by default and allows only authorized communications;<br>(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;<br>(e) Protect the authenticity of communications sessions;<br>(f) Invalidate session identifiers upon logout or other session termination; and<br>(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:<br>(a) Protect information in transit between systems;<br>(b) Protect information at rest in the system; and<br>(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:<br>(a) Employ malicious code protection mechanisms at entry and exit points to the Solution that can detect and eradicate malicious code;<br>(b) Maintain the malicious code protection mechanisms in an up-to-date state in accordance with organizational configuration management policies; and<br>(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:<br>(a) Be able to detect attacks, indicators of potential attacks and unauthorized local, network, and remote connections; and<br>(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:<br>(a) The port, protocol, or service being used;<br>(b) A description of the information being transferred in that port/protocol/service;<br>(c) A description of the flow (source and destination); and<br>(d) Any firewall or routing rules necessary to support the communication. |
| Security Testing | SC.27 | The Contractor must:<br>(a) Create and implement a security assessment plan;<br>(b) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;<br>(c) Implement a verifiable flaw remediation process; and<br>(d) Correct flaws identified during security testing/evaluation.<br>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 for PB/H/M. |
| 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 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. |
| 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:<br>(a) Threats and vulnerabilities; and<br>(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 for PB/H/M. |
| | 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:<br>(a) The security functions to be tested;<br>(b) GC witnessing the testing arrangements; and<br>(c) For each security function or sets of security functions, the items to be tested, including:<br>i. A description of the test case, procedure, or scenario;<br>ii. Environmental requirements;<br>iii. Ordering dependencies; and<br>iv. Expected results (i.e., pass/fail criteria). |
| | SC.43 | The Solution must maintain data integrity during conversion between various protocols and data formats**.** |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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:<br>(a) For each Privileged User role:<br>i. Schedule of security-relevant actions to be performed in order to maintain the security posture of the ISS;<br>ii. How to use available operational interfaces; and<br>iii. Each scheduled action and how the User is expected to perform it.<br>(b) Operational roles and responsibilities for:<br>i. Interaction requirements with PWGSC representatives;<br>ii. Reporting schedule and procedures;<br>iii. Access control;<br>iv. Audit and accountability;<br>v. Identification and authentication;<br>vi. System and communications protection;<br>vii. Awareness and training;<br>viii. Configuration management;<br>ix. Contingency planning;<br>x. Incident response;<br>xi. Maintenance;<br>xii. Media protection;<br>xiii. Physical and environment protection;<br>xiv. Personnel security; and<br>xv. System and information integrity. |
| | SC.48 | The Contractor must provide detailed Security Installation Procedures to GC that include, at a minimum:<br>(a) Steps necessary for the secure installation and configuration;<br>(b) Installation and configuration of all technical security solutions;<br>(c) Security configuration of Hardware products; and<br>(d) Security configuration of software products. |

| 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:<br>(a) The security verification approach;<br>(b) The GC witnessing arrangements;<br>(c) An outline of the security verification items; and<br>(d) For each security verification item:<br>i. A description of the verification scenario;<br>ii. Ordering dependencies;<br>iii. Expected results (i.e., pass/fail criteria);<br>iv. Actual results; and<br>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:<br>(a) The expected results (i.e., pass/fail criteria);<br>(b) The actual results; and<br>(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:<br>(a) The security requirement identifier;<br>(b) An identifier that maps the security requirement to the corresponding statement in the ANNEX A (e.g., heading or line identifier);<br>(c) The security requirement statement;<br>(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;<br>(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);<br>(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;<br>(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<br>(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:<br>(a) Logout user-initiated communications sessions whenever authentication is used; and<br>(b) Display an explicit logout message to users indicating the reliable termination of authenticated communications sessions. |
| Security Attributes | SC.63 | The Solution must have mechanisms to maintain the association and integrity of GC-defined security attributes. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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<br>(a) Bind the identity of the information producer with the information to the GC defined strength of binding and;<br>(b) Provide the means for authorized individuals to determine the identity of the producer of the information. |
| | SC.69 | The Solution must<br>(a) Validate the binding of the information producer identity to the information at the frequency defined by the GC; and<br>(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<br>(a) Privileged accounts; and<br>(b) Non-privileged accounts. |
| Authenticator Management | SC.71 | DELETED |
| 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. |
| Access Control and Account Management | SC.75 | When creating operating documentation for the business, the Contractor will have to include the process(es) that describe the management of the roles and user access controls. These are to be documented by the Contractor in an Access Control and User Management Plan and can serve as SA&A evidence. |

# SECTION 6: TESTING MANAGEMENT

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.00.A | Prepare a Preliminary Testing Plan in accordance with the requirements of ANNEX A, Section 6. The Contractor should be guided by the business and technical requirements and conceptual architecture for preparing the test plan. |
| | TM.01.A | Before commencement of the development Work, the Contractor must develop the Testing Strategy. Subject to the approval of the Project Authority, the Strategy must include, as a minimum but not limited to, the following information for all stages of the required testing:<br>(a) A high-level of overview of the proposed testing strategy;<br>(b) A Defect Management Framework;<br>(c) Entry and exit strategy;<br>(d) Meetings between the Contractor and Project Authority; and<br>(e) On-going risk management and mitigation strategy. |
| | TM.01.B | The Contractor must develop a Testing Plan which demonstrates, but is not limited to:<br>A. Due consideration of related Security requirements from SC-42 Security Integration Test Plan as well as Section 6 of ANNEX A;<br>B. Adequate test coverage to ensure Solution go-live readiness. Due consideration of and reference to :<br>i. Integration testing;<br>ii. Functional and non-functional Testing, including Security Testing;<br>iii. Data Validation Testing;<br>iv. Client acceptance testing.<br>C. The identification of risk and its management. |
| | 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:<br>(a) An ongoing log of all defects found during testing of the solution; and<br>(b) Descriptions of defect, level of severity, stage of testing discovered, actions taken to resolve, and current status.<br>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:<br>(a) A summary of actions performed in the past week as well as next steps in the testing stage; and |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | (b) The most recent copy of defect tracking report.<br>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.06.A | Provide the completed Requirements Traceability Matrix. |
| | 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 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:<br>(a) Conduct Unit Testing, Path Analysis, System, Integration and Functional Testing on each module or component of the Solution;<br>(b) Create and provide Test Scripts;<br>(c) Log all defects found before performing the next-stage testing; and<br>(d) Ensure testing cycles continue until a full cycle is completed with minimal bugs or acceptable defects, approved by the Project Authority.<br>The completion of testing is subject to the final approval of the Project Authority. |
| | TM.10 | The Contractor must:<br>(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);<br>(b) Develop and provide Testing Scripts (including Regression testing);<br>(c) Ensure that the testers have the ability to log defects, bugs and anomalies whether part of a documented test case or not;<br>(e) Ensure testing cycles continue until a full cycle is completed with minimal bugs or acceptable defects, as approved by the Project Authority;<br>(d) The Contractor must log and address all testing defects before final-sign off can be obtained from the Project Authority. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | 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: MANAGEMENT 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 (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.

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 MANAGEMENT

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 MANAGEMENT

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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | PM.03 | The Contractor must deliver all softcopy documentation to the Project Authority in the following formats:<br>(a) Text documents or presentations using Microsoft Office (Word, PowerPoint, Excel), version 2013 or later;<br>(b) Diagrams and flowcharts: Microsoft Visio, version 2013 or later; and<br>(c) Project plans and schedules: Microsoft Project, version 2013 or later.<br>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:<br>(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;<br>(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;<br>(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<br>(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.<br>(e) All project work where the Contractor requires direct access to ISS information and assets will be required to be done on-site for the duration of the work. Once the required work has been completed those resources are no longer required to be on-site.<br>(f) Except where otherwise specified, all project work that does not require direct access to ISS information and assets can be done off-site. |
| 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.05.A | The Contractor must prepare a Preliminary Project Management Plan that reflects their 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. |
| | PM.06 | 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | The Plan must respond to the following requested elements and indicate how they support the intended outcomes listed in ANNEX A, Section 1 and 7, including:<br>(a) Project Governance and Team Structure Document;<br>(b) Scope Management Plan;<br>(c) Schedule Management Plan;<br>(d) Project Schedule;<br>(e) Risk Management Plan; and<br>(f) Quality Management Plan. |
| Project Schedule | PM.07 | The Contractor must:<br>(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;<br>(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<br>(c) Identified changes to the Project Schedule as a result of Change Requests are to be incorporated into the project Risk Register.<br>(d) Update the Project Schedule as the required during the project's progression or 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:<br>(a) Number of the action item;<br>(b) Description of the action item;<br>(c) Person responsible for following through (OPI);<br>(d) Date Initiated;<br>(e) Date due;<br>(f) Status;<br>(g) Percentage of Completion vs Baseline schedule; and<br>(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:<br>(a) Subject;<br>(b) Date of meeting;<br>(c) Time of meeting;<br>(d) Place of meeting;<br>(e) Required attendees;<br>(f) Optional attendees;<br>(g) Action Items listed to be reviewed /discussed; and |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | (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:<br>(a) Meeting Title;<br>(b) Date and time of meeting;<br>(c) Attendees and absentees;<br>(d) Minutes taken by;<br>(e) Copy of minutes sent to;<br>(f) Minutes of discussions;<br>(g) Record of decisions taken;<br>(h) Action items raised;<br>(i) Other business; and<br>(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 a weekly or as required basis and include the following information, at a minimum:<br>(a) Milestone Status;<br>(b) Status and issues information relating to completion dates;<br>(c) Identify any new risks to deliverables and outline mitigation strategies for risks already identified; and<br>(d) Any requests for change. |
| | PM.12 | The Contractor must provide Change Request Management Procedures to GC that includes, at a minimum:<br>(a) Contractor resource roles and responsibilities for change request management;<br>(b) How the Contractor will use the change request management process to support the development of the Solution;<br>(c) Method used to uniquely identify configuration items;<br>(d) Configuration item identification method;<br>(e) Description of the change request management process, including the change review and approval process;<br>(f) Means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items;<br>(g) Measures used to enforce only authorized changes;<br>(h) Procedures that the Contractor will use to accept modified or newly created configuration items; and<br>(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 |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | Register must be provided as required or requested by the Project Authority. At a minimum the Project Risk Register must include:<br>(a) Id #;<br>(b) Description;<br>(c) Response/Mitigation Strategy; and<br>(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:<br>(a) Id #;<br>(b) Description;<br>(c) Response/Mitigation Strategy; and<br>(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 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:<br>(a) Assessment of project performance;<br>(b) Identification of lessons learned;<br>(c) Confirmation that essential contractual and other project closure activities have been completed;<br>(d) Outstanding Issues;<br>(e) Transfer of assets, deliverables and ongoing administrative functions; and<br>(f) Measurement of post implementation benefits/outcomes (KPI) delivered by the project. |

## 2.1 REQUIREMENT OVERVIEW - CHANGE MANAGEMENT

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 MANAGEMENT

### 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. |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | 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:<br>(a) Assessment to understand the:<br>i. Change (Context of Change, Impact of Change, Change Agility [readiness]);<br>ii. Project;<br>iii. Change risk assessment;<br>iv. Stakeholder identification and mapping;<br>v. Stakeholder required knowledge/skills; and<br>vi. Organizational changes identifying key areas of change and potential impacts.<br>(b) Communication strategy based on identified areas of change and impacted stakeholders;<br>(c) Training strategy based on identified areas of change and impacted stakeholders;<br>(d) A Gap Analysis to identify required areas of Engagement, Communications and Training;<br>(e) "Best Fit Change Strategy" that identifies the right overall concept for delivering change based on the assessment. This should cover benefits of the approach, how to involve stakeholders, sustainability and assessment of operational readiness;<br>(f) Discussion of transition approach based on leading practices;<br>(g) Transitional success criteria and how transitional success will be evaluated;<br>(h) Identification of change levers available to the project team;<br>(i) Change resourcing expectations based on project phases and milestones; and<br>(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.01.A | The Contractor must prepare a Preliminary Change Management Plan which includes, but is not limited to:<br>A. A comprehensive understanding of the Change Management requirements;<br>B. Consideration of the following:<br>i. Avoidance of disruption of service to Canadians; |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | ii. Facilitation of the adoption of process and terminology transitions for all end users, including external users and internal staff;<br>iii. Appropriate, accurate and timely use and input to the new system; and<br>iv. The quality and integrity of the services rendered.<br>A comprehensive evaluation method for assessing effectiveness of change management activities. |
| | CM.02 | The Contractor must prepare a Change Management Plan after the Preliminary Change Management Plan has been evaluated by Canada and deemed that the plan supports the successful transition from “as-is” to “to be” states and demonstrates the requirements identified above.<br>The Change Management Plan must be integrated with the Project Management Plan and Project Schedule. |
| | CM.03 | The Contractor must:<br>(a) Develop processes and procedures to institutionalize the change;<br>(b) Identify change management activities and link them to project milestones<br>(c) Align with training timelines, communications, and approaches;<br>(d) Align with process re-engineering transition activity timelines;<br>(e) Identify change resourcing expectations based on project phases and milestones;<br>(f) Identify when, for how long, and the type of GC resources that are required for change management;<br>(g) Identify high risk areas that might impact successful change, develop mitigation strategies and recommended mitigation actions, and report results to GC;<br>(h) Identify quick wins for simplifying change management activities;<br>(i) Work in collaboration with the GC in executing the Change Management Strategy and Plan;<br>(j) Action change management remediation activities required throughout project lifecycle;<br>(k) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues;<br>(l) Support identified GC Change Management resources who will champion change;<br>(m) Coordinate between the various components of change management and the other project activities; and<br>Provide an in service support plan which includes knowledge transfer for operations. |
| 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:<br>(a) Assessment of current operations<br>(b) Criteria for determining readiness to change<br>(c) Assessment of readiness at the start of development<br>(d) Reassessment of change management progress and operational readiness as the project progresses and prior to each go live; and |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | (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:<br>(a) Overview of content for communication artifacts such as but not limited to:<br>i) Communicating the benefits of the ISST project;<br>ii) Communicating how the GC readiness activities will be accomplished;<br>iii) Communicating how Users can support the GC;<br>iv) Transition effort to migrate from the current AS-IS business processes and system to the future TO-BE business processes and system;<br>v) Post-migration assessment to aid in future transition activities; and<br>vi) A timeline and key messages and mediums for each stage of the project.<br>(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;<br>(c) Develop a change advocate network within ISS to facilitate leadership engagement for active support and driving of change;<br>(d) Identifying communication activities throughout the lifecycle of the project, flagging any potential obstacles to initiating those activities and possible solutions; and<br>(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:<br>(a) Evaluate and update communication activities based on project risks and issues and provide assessment on what communication activities can assist in mitigation measures;<br>(b) Facilitate workshops to discuss, analyze and validate changes;<br>(c) Deliver information sessions including, but not limited to: proof of concept sessions, hands on system trials, brainstorming sessions, etc.;<br>(d) Document feedback from communications to produce a report outlining successfulness of delivered communication activities;<br>(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.;<br>(f) Reassess communication activities based on readiness assessments and report findings and provide recommendations: and<br>(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.<br>(a) As a minimum, the Training Plan must describe the training approach, as well as how the Contractor will: |

| Category | SOW NUM | Requirement |
|---|---|---|
| | | i) Define required skills and level of skills to support the application in terms of business knowledge, application knowledge and solution knowledge;<br>ii) Articulate how Users will be assessed to ensure they have an understanding of their roles and the solutions capabilities;<br>iii) Identify methods, procedures and materials required for delivering training, user acceptance testing and knowledge transfer;<br>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;<br>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;<br>(b) As a minimum, the Training Plan for Users must:<br>i) Include a schedule of training phases beginning early in 2018 and continuing through to March 2019;<br>ii) Clearly outline training needs;<br>iii) Clearly outline training delivery methods and materials specific to each user type;<br>iv) Articulate how users will be assessed to ensure they have an understanding of their roles and system capabilities;<br>v) Identify required skills and competency levels to support the application in terms of business knowledge, application knowledge and solution knowledge;<br>vi) Link the communication of training activities to the Change Management Communication Plan;<br>vii) Synchronize scheduled training activities to account for Process Re-Engineering activities;<br>viii) Include instructions on locating training resources;<br>ix) Detail expected User outcomes; and<br>x) Detail instructions on each transition approach including:<br>(1) Tools and resources that will be available;<br>(2) How to populate User profiles;<br>(3) Frequently asked questions; and<br>(4) Instructions on providing feedback during the transition.<br>(c) As a minimum, the Training Plan for level 2 service desk agents must include:<br>i) Schedule of transition activities;<br>ii) Description of access rights and roles and responsibilities of level 1 service desk agents during the GC migration;<br>iii) Instructions on locating training resources; and<br>iv) Escalation procedures.<br>(d) As a minimum, the Training Plan for Authorized Administrators must include:<br>i) Schedule of transition activities;<br>ii) Description of access rights and roles and responsibilities of GC and GC Administrators during the GC migration; and<br>iii) Instructions on locating training resources. |

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

# 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.

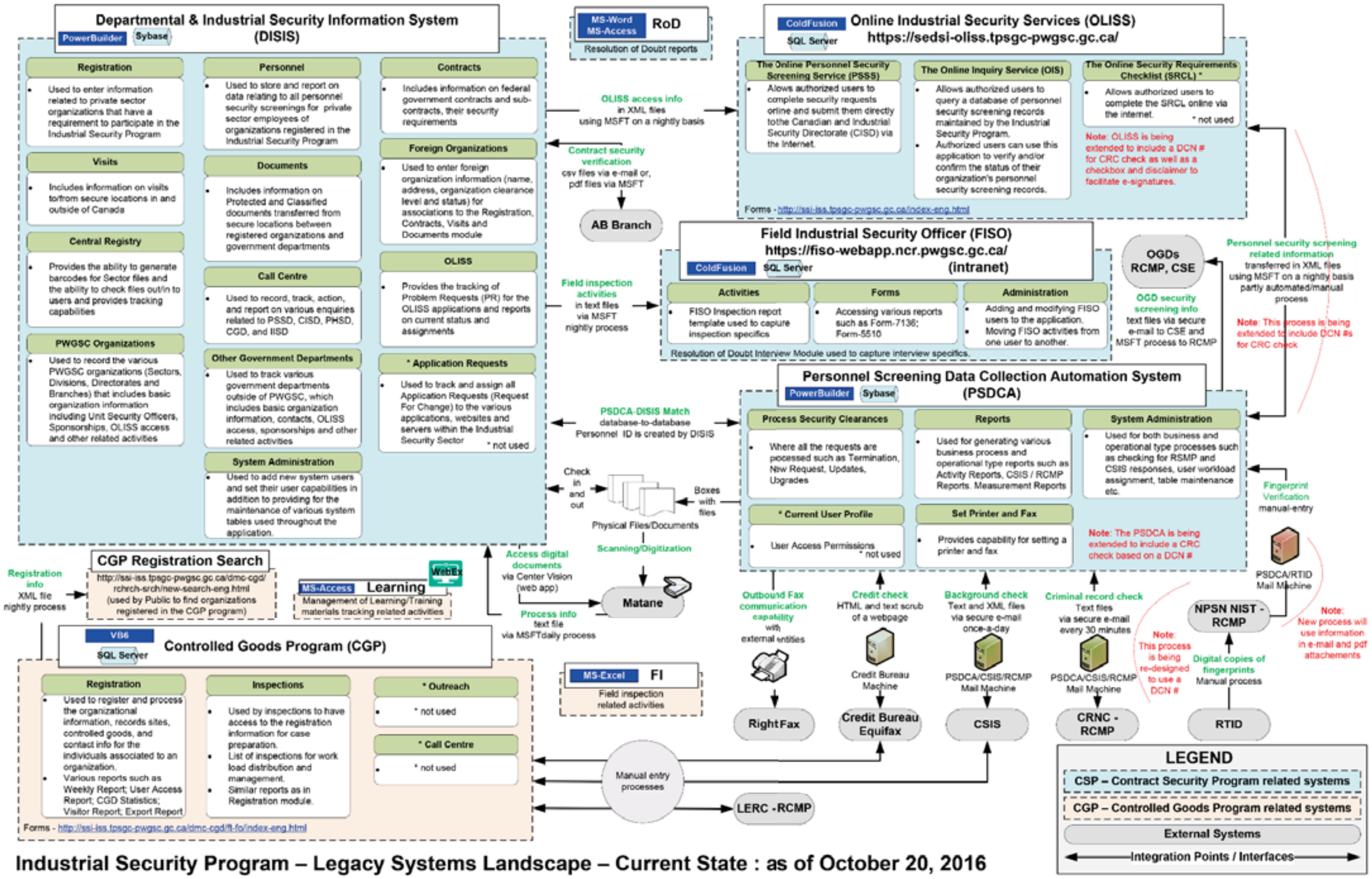
## 1.8 ADDITIONAL SECURITY SERVICES

In addition to the Security services described in Section 5: IT Security Requirements, the Contractor must, on an as-and-when basis, provide additional IT Security services and must propose resources that are qualified and have experience providing IT Security services.

# 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.



**Departmental & Industrial Security Information System (DISIS)** PowerBuilder Sybase

**Registration**
- Used to enter information related to private sector organizations that have a requirement to participate in the Industrial Security Program

**Visits**
- Includes information on visits to/from secure locations in and outside of Canada

**Central Registry**
- Provides the ability to generate barcodes for Sector files and the ability to check files out/in to users and provides tracking capabilities

**PWGSC Organizations**
- Used to record the various PWGSC organizations (Sectors, Divisions, Directorates and Branches) that includes basic organization information including Unit Security Officers, Sponsorships, OLISS access and other related activities

**Personnel**
- Used to store and report on data relating to all personnel security screenings for private sector employees of organizations registered in the Industrial Security Program

**Documents**
- Includes information on Protected and Classified documents transferred from secure locations between registered organizations and government departments

**Call Centre**
- Used to record, track, action, and report on various enquiries related to PSSD, CISD, PHSD, CGD, and IISD

**Other Government Departments**
- Used to track various government departments outside of PWGSC, which includes basic organization information, contacts, OLISS access, sponsorships and other related activities

**System Administration**
- Used to add new system users and set their user capabilities in addition to providing for the maintenance of various system tables used throughout the application.

**Contracts**
- Includes information on federal government contracts and sub-contracts, their security requirements

**Foreign Organizations**
- Used to enter foreign organization information (name, address, organization clearance level and status) for associations to the Registration, Contracts, Visits and Documents module

**OLISS**
- Provides the tracking of Problem Requests (PR) for the OLISS applications and reports on current status and assignments

*** Application Requests**
- Used to track and assign all Application Requests (Request For Change) to the various applications, websites and servers within the Industrial Security Sector * not used

**RoD** MS-Word MS-Access
Resolution of Doubt reports

**Online Industrial Security Services (OLISS)** ColdFusion SQL Server
https://sedsi-oliss.tpsgc-pwgsc.gc.ca/

**The Online Personnel Security Screening Service (PSSS)**
- Alows authorized users to complete security requests orline and submit them directly tothe Canadian and Industrial Security Directorate (CISD) via the Internet.

**The Online Inquiry Service (OIS)**
- Allows authorized users to query a database of personnel security screening records maintained by the Industrial Security Program.
- Authorized users can use this application to verify and/or confirm the status of their organization's personnel security screening records.

**The Online Security Requirements Checklist (SRCL) ***
- Allows authorized users to complete the SRCL online via the internet. * not used

Note: OLISS is being extended to include a DCN # for CRC check as well as a checkbox and disclaimer to facilitate e-signatures.

Forms - http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html

**Field Industrial Security Officer (FISO)** ColdFusion SQL Server
https://fiso-webapp.ncr.pwgsc.gc.ca/ (intranet)

**Activities**
- FISO Inspection report template used to capture inspection specifics

**Forms**
- Accessing various reports such as Form-7136; Form-5510

**Administration**
- Adding and modifying FISO users to the application.
- Moving FISO activities from one user to another.

Resolution of Doubt Interview Module used to capture interview specifics.

**Personnel Screening Data Collection Automation System (PSDCA)** PowerBuilder Sybase

**Process Security Clearances**
- Where all the requests are processed such as Termination, New Request, Updates, Upgrades

**Reports**
- Used for generating various business process and operational type reports such as Activity Reports, CSIS / RCMP Reports, Measurement Reports

**System Administration**
- Used for both business and operational type processes such as checking for RSMP and CSIS responses, user workload assignment, table maintenance etc.

*** Current User Profile**
- User Access Permissions * not used

**Set Printer and Fax**
- Provides capability for setting a printer and fax

Note: The PSDCA is being extended to include a CRC check based on a DCN #

OLISS access info in XML files using MSFT on a nightly basis

Contract security verification csv files via e-mail or, pdf files via MSFT

AB Branch

Field inspection activities in text files via MSFT nightly process

PSDCA-DISIS Match database-to-database Personnel ID is created by DISIS

Check in and out

Boxes with files

Physical Files/Documents

Scanning/Digitization

Access digital documents via Center Vision (web app)

Matane

Process info text file via MSFTdaily process

OGDs RCMP, CSE

OGD security screening info text files via secure e-mail to CSE and MSFT process to RCMP

Personnel security screening related information transferred in XML files using MSFT on a nightly basis partly automated/manual process

Note: This process is being extended to include DCN #s for CRC check

Fingerprint Verification manual-entry

PSDCA/RTID Mail Machine

Note: New process will use information in e-mail and pdf attachements

NPSN NIST - RCMP

Digital copies of fingerprints Manual process

RTID

Note: This process is being re-designed to use a DCN #

Outbound Fax communication capability with external entities

RightFax

Credit check HTML and text scrub of a webpage

Credit Bureau Machine

Credit Bureau Equifax

Background check Text and XML files via secure e-mail once-a-day

PSDCA/CSIS/RCMP Mail Machine

CSIS

Criminal record check Text files via secure e-mail every 30 minutes

PSDCA/CSIS/RCMP Mail Machine

CRNC - RCMP

Manual entry processes

LERC - RCMP

**FI** MS-Excel
Field inspection related activities

**CGP Registration Search**
http://ssi-iss.tpsgc-pwgsc.gc.ca/dmc-cgd/rchrch-srch/new-search-eng.html (used by Public to find organizations registered in the CGP program)

Registration info XML file nightly process

**Learning** MS-Access WebEx
Management of Learning/Training materials tracking related activities

**Controlled Goods Program (CGP)** VB6 SQL Server

**Registration**
- Used to register and process the organizational information, records sites, controlled goods, and contact info for the individuals associated to an organization.
- Various reports such as Weekly Report; User Access Report; CGD Statistics; Visitor Report; Export Report

**Inspections**
- Used by inspections to have access to the registration information for case preparation.
- List of inspections for work load distribution and management.
- Similar reports as in Registration module.

*** Outreach**
- * not used

*** Call Centre**
- * not used

Forms - http://ssi-iss.tpsgc-pwgsc.gc.ca/dmc-cgd/fi-fo/index-eng.html

**LEGEND**

CSP – Contract Security Program related systems

CGP – Controlled Goods Program related systems

External Systems

Integration Points / Interfaces

**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<br>• Industrial Security Sector Contract Security Program – Contract Analyst |
| Business Objective | • Submission of SRCL by Contracting Authority for analysis and provision of security clauses.<br>• 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.<br>2. Client contract authority identifies that the contract has possible security requirements.<br>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.<br>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.<br>6. If it is a new SRCL, a new entry is created into the existing supporting application. Go to step 16.<br>7. If it is revision to an existing SRCL, the existing SRCL and contract information is retrieved. Go to step 16.<br>8. If is a sub-SRCL the CSP will validate that the primary contract exists and is at the appropriate security level.<br>9. If the sub-SRCL's primary contract does not exist, the sub-SRCL is rejected.<br>10. The client authority who submitted the sub-SRCL is notified of the rejection. Go to step 15.<br>11. If the sub-SRCL's primary contract does exist, the CSP will confirm if the primary contract has been approved.<br>12. If the sub-SRCL's primary contract has not been approved, the contract authority and company security officer (CSO) are notified.<br>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.<br>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.<br>15. The contract pre award process ends.<br>16. The CSP reviews the submitted SRCL and any supplied supporting documentation.<br>17. The CSP reviews the submitted SRCL for completeness.<br>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.<br>19. If the SRCL is complete, the CSP identifies the required domestic security clauses based on the contracts security requirements.<br>20. If the SRCL indicates there are foreign security requirements. The International Industrial Security Directorate (IISD) is consulted.<br>21. The IISD identifies the required foreign security clauses and supplies them back to the CSP.<br>22. The CSP returns all identified security clauses to the client authority for inclusion into the contract's RFP.<br>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.<br>24. The client authority adds the supplied security clauses to the contract solicitation documentation.<br>25. The contract is placed for RFP.<br>26. Contract potential bidders are identified.<br>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.<br>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<br>• 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<br>• 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.<br>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).<br>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.<br>5. If the supplied information is complete, the CSP verifies if the contract is compliant.<br>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.<br>7. If the security clauses are missing from the contract.<br>8. The CSP contacts the client contract authority advising of required action. Go to step 30.<br>9. If there is a noted security breach, the CSP will check with the client contract authority for breach mitigations.<br>10. If the CSP is satisfied with the client contract authority response, go to step 30.<br>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.<br>12. If the awarded contractor requires to be registered with the CSP.<br>13. The client contract authority is notified that the contracting organization needs to be registered.<br>14. The CSP registration process is triggered (3 WF CSP Registration New/Upgrade). Go to step 18.<br>15. If the awarded contractor is already registered but requires an upgrade to their security clearance level.<br>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.<br>17. The CSP registration upgrade process is triggered (3 WF Registration New/Upgrade). Go to step 18.<br>18. If the contracting organization is found to be compliant as part of the registration process, go to step 23.<br>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.<br>20. If all compliancy issues were resolved, go to step 23.<br>21. If all compliancy issues were not resolved, after a predetermined number of attempts with no response, the contract is closed-out.<br>22. An investigation is triggered (12 WF CSP Investigations). Go to step 30.<br>23. Interested stakeholders such as Communications Security Establishment Canada (CSEC), ISS Controlled Goods Program (CGP), etc. are notified of the contract award.<br>24. If the contract has inspection requirements such as an IT inspection. If there are no inspection requirements go to step 28.<br>25. The contract analyst will initiate an inspection<br>26. The inspection process occurs (10 WF CSP Inspection).<br>27. If the inspection process identified any issues, the contract is followed up on.<br>28. If identified issues were not resolved, the contract is followed up on again, this cycle continues until all inspection identified issues are resolved.<br>29. If all identified issues are resolved, the client contract authority is advised to proceed with the processing of the contract.<br>30. The process ends. |
| Inputs | • Security Requirements Check List (SRCL)<br>• Awarded contract and supplemental information |

| | |
|---|---|
| | • Investigation results<br>• Inspection results<br>• Organization Registration New or Upgrade |
| Outputs | • Close out of contract for non-compliancy<br>• Stakeholder notifications<br>• 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<br>• CSP Contract Analyst<br>• CSP Registration Clerk<br>• CSP Registration Analyst |
| Business Objective | • To perform security screening of new registered organizations to ensure contract security.<br>• 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.<br>• CSP Contract Analyst triggers the registration process. |

| | |
|---|---|
| Workflow Description | 1. Start of process.<br>2. Sponsoring organization or CSP contract analyst submits a request to register a new organization or upgrade an existing organization.<br>3. CSP registration clerk verifies if the organization already exists within the contract security program.<br>4. If the organization already exists, the CSP registration clerk verifies if the requested security level is greater than the organizations current security level.<br>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.<br>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.<br>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.<br>8. The sponsor is sent a rejection letter.<br>9. The registration request is closed-out.<br>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.<br>11. CSP registration analyst reviews the registration package. If the registration package is complete, go to step 17.<br>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.<br>13. If the documentation is provide within 30 business days, go to step 17.<br>14. If the requested documentation is not provided within 30 business days, a follow-up on the establishing letter is sent to the organization.<br>15. If the requested documentation is provided within 5 business days, go to step 17.<br>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.<br>17. The CSP registration analyst reviews and validates all provided information.<br>18. If the organization security clearance is for a Designated Organizational Screening (DOS).<br>19. The DOS security clearance process is triggered (4 WF CSP Registration DOS).<br>20. If the organization security clearance is for Facility Security Clearance (FSC).<br>21. The FSC security clearance process is triggered (5 WF CSP Registration FSC).<br>22. If the organization security clearance is for Document Safeguarding Capability (DSC).<br>23. The FSC security clearance process is triggered (6 WF CSP Registration DSC).<br>24. The registration new/upgrade process ends. |
| Inputs | • PSOS<br>• Supplied organization information |
| Outputs | • Establishing letter<br>• 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<br>• CSP Registration Quality Assurance Officer<br>• CSP Registration Chief |
| Business Objective | • To clear an organization at the DOS security clearance level. |
| Trigger | • New or upgrade registration request.<br>• FSC or DSC registration request. |
| Workflow Description | 1. Start of process.<br>2. CSP registration analyst confirms that all required information is received.<br>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.<br>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.<br>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).<br>7. The registration package is returned from PSSD and the PSS results are reviewed.<br>8. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 5.<br>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.<br>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.<br>11. If there is nothing preventing the organization termination, as required all PSS clearances are terminated.<br>12. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination.<br>13. The registration request is closed-out for non-compliance. Go to step 21.<br>14. CSP registration analyst creates the notification of registration.<br>15. The file is submitted to the CSP quality assurance officer for review.<br>16. CSP quality assurance officer reviews the file.<br>17. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates.<br>18. CSP registration analyst updates the file, go to step 15.<br>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.<br>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.<br>21. The trigger for the DOS can trigger other registration processes.<br>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).<br>23. Where required, the new or upgrade registration process may be triggered (3 WF CSP Registration New/Upgrade). |
| Inputs | • PSOS<br>• Establishing letter<br>• Supplied organization information<br>• PSSD results |
| Outputs | • Termination notice<br>• PSSD registration package<br>• Granting letter<br>• Organization clearance letter<br>• PSS briefing forms<br>• 3G security agreement<br>• Organizational security status |

### 1.1.4.2 Facility Safeguarding Capability

| Workflow ID | 5 WF CSP Registration FSC |
|---|---|
| Business Unit(s) | • CSP Registration Analyst<br>• CSP Registration Quality Assurance Officer<br>• CSP Registration Chief |
| Business Objective | • To clear an organization at the FSC security clearance level. |
| Trigger | • New or upgrade registration request.<br>• DOS registration request. |
| Workflow Description | 1. Start of process.<br>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.<br>3. If there is a requirement to process a DOS security clearance, the DOS clearance process is triggered (4 WF CSP Registration DOS).<br>4. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 8.<br>5. If there are organizational changes the CSP registration analyst reviews in detail the organization.<br>6. CSP registration analyst performs a call briefing with the organizations CSO.<br>7. The CSP registration analyst completed a 1A Requirements report.<br>8. CSP registration analyst verifies that all information is received.<br>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.<br>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.<br>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.<br>12. The PSS process is triggered (13 WF CSP PSS Request).<br>13. The registration package is returned from PSSD and the PSS results are reviewed.<br>14. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 11.<br>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.<br>17. If there is nothing preventing the organization termination, as required all PSS clearances are terminated.<br>18. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination.<br>19. The registration request is closed-out for non-compliance or the security clearance is downgraded to DOS. Go to step 27.<br>20. CSP registration analyst creates the notification of registration.<br>21. The file is submitted to the CSP quality assurance officer for review.<br>22. CSP quality assurance officer reviews the file.<br>23. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates.<br>24. CSP registration analyst updates the file, go to step 21.<br>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.<br>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.<br>27. The trigger for the FSC can trigger other registration processes.<br>28. Where required, a Document Safeguarding Capability (DSC) would be triggered (6 WF CSP Registration DSC).<br>29. Where required, the new or upgrade registration process may be triggered (2 WF CSP Registration New/Upgrade). |
| Inputs | • PSOS<br>• Establishing letter<br>• Supplied organization information<br>• PSSD results |
| Outputs | • Termination notice<br>• PSSD registration package<br>• Granting letter<br>• Organization clearance letter<br>• PSS briefing forms<br>• 3G security agreement<br>• Organizational security status |

### 1.1.4.3 Document Safeguarding Capability

| Workflow ID | 6 WF CSP Registration DSC |
|---|---|
| Business Unit(s) | • CSP Registration Analyst<br>• Canadian Industrial Security Directorate (CISD) Director |
| Business Objective | • To clear an organization at the DSC security clearance level. |
| Trigger | • New or upgrade registration request.<br>• DOS registration request. |
| Workflow Description | 1. Start of process.<br>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.<br>3. If there is a requirement to process a DOS security clearance, the DOS clearance process is triggered (4 WF CSP Registration DOS).<br>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.<br>5. If there is a requirement to process a FSC security clearance, the FSC clearance process is triggered (5 WF CSP Registration FSC).<br>6. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 9.<br>7. If there are organizational changes the CSP registration analyst reviews in detail the organization.<br>8. CSP registration analyst performs a call briefing with the organizations CSO.<br>9. CSP registration analyst determines if parent exclusion is required. If no parent exclusion is required, go to step 13.<br>10. If there is parent exclusion, the CSP analyst requests additional information from the organization.<br>11. CSP registration analyst reviews and analyzes the received information.<br>12. Approval of the organization's parent exclusion is provided by the CISD director.<br>13. CSP registration analyst verifies that all information is received.<br>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.<br>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.<br>17. The PSS process is triggered (3 WF CSP PSS Request).<br>18. The registration package is returned from PSSD and the PSS results are reviewed.<br>19. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 16.<br>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.<br>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.<br>22. If there is nothing preventing the organization termination, as required all PSS clearances are terminated.<br>23. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination.<br>24. The registration request is closed-out for non-compliance. Go to step 27.<br>25. CSP registration analyst creates an inspection request.<br>26. The inspection process is triggered (10 WF CSP Inspection).<br>27. Where required, the new or upgrade registration process may be triggered (3 WF CSP Registration New/Upgrade). |
| Inputs | • PSOS<br>• Establishing letter<br>• Supplied organization information<br>• PSSD results |
| Outputs | • Termination notice<br>• PSSD registration package<br>• Granting letter<br>• Organization clearance letter<br>• PSS briefing forms<br>• 3G security agreement<br>• 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<br>• Registration Clerk<br>• CSP Registration Analyst<br>• CSP Registration Quality Assurance Officer<br>• CSP Registration Chief |
| Business Objective | • To renew an organizations security clearance. |
| Trigger | • Organization renewal requirement. |
| Workflow Description | 1. Start of process.<br>2. CSP registration clerk pulls report of expiring organizations.<br>3. CSP registration clerk notifies organization of renewal requirement.<br>4. Registered organization submits renewal information.<br>5. CSP registration clerk reviews, prioritizes and assigns request to registration analyst.<br>6. CSP registration clerk determines if to continue with renewal. If there is a need to continue, go to step 8.<br>7. If there is no need to continue with the renewal, close out the request for non-compliance.<br>8. CSP registration analyst reviews and validates the renewal information.<br>9. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 15.<br>10. If there are organizational changes the CSP registration analyst reviews in detail the organization.<br>11. CSP registration analyst determines if there are any DSC requirements. If there are not any DSC requirements, go to step 14.<br>12. CSP registration analyst submits an inspection request.<br>13. The inspection process is triggered (10 WF CSP Inspection).<br>14. CSP registration analyst performs a call briefing with the organizations CSO.<br>15. CSP registration analyst verifies that all information is received.<br>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.<br>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.<br>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.<br>20. The registration package is returned from PSSD and the PSS results are reviewed.<br>21. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 18.<br>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.<br>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.<br>24. If there is nothing preventing the organization termination, as required all PSS clearances are terminated.<br>25. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination.<br>26. The registration request is closed-out for non-compliance or the security clearance is downgraded to DOS. Go to step 34.<br>27. CSP registration analyst creates the notification of renewal.<br>28. The file is submitted to the CSP quality assurance officer for review.<br>29. CSP quality assurance officer reviews the file.<br>30. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates.<br>31. CSP registration analyst updates the file, go to step 28.<br>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.<br>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.<br>34. The process ends. |
| Inputs | • Renewal information<br>• PSSD results |
| Outputs | • Termination notice<br>• Granting letter<br>• Organization clearance letter<br>• PSS briefing forms<br>• 3G security agreement<br>• 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<br>• CSP Contract Analyst<br>• Registered Organization<br>• CSP Registration Clerk<br>• CSP Registration Analyst<br>• CSP Registration Quality Assurance Officer<br>• CSP Registration Chief |
| Business Objective | • To update an organizations information for security clearance. |
| Trigger | • Organization update requirement. |
| Workflow Description | 1. Start of process.<br>2. Sponsoring organization or CSP contract analyst submits update to an organization’s information.<br>3. Registered organization submits an update to their information.<br>4. CSP registration clerk reviews, prioritizes and assigns request to registration analyst.<br>5. CSP registration clerk determines if to continue with update. If there is a need to continue, go to step 8.<br>6. If there is no need to continue with the update, reject the update request.<br>7. CSP registration clerk notifies the CSO of the rejected update. Go to step 34.<br>8. CSP registration analyst reviews and validates the update information.<br>9. CSP registration analyst reviews the organization for any corporate changes. If there are no corporate changes, go to step 15.<br>10. If there are organizational changes the CSP registration analyst reviews in detail the organization.<br>11. CSP registration analyst determines if there are any DSC requirements. If there are not any DSC requirements, go to step 14.<br>12. CSP registration analyst submits an inspection request. |

| | |
|---|---|
| | 13. The inspection process is triggered (10 WF CSP Inspection). Go to step 34.<br>14. CSP registration analyst performs a call briefing with the organizations CSO.<br>15. CSP registration analyst verifies that all information is received.<br>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.<br>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.<br>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.<br>19. The PSS process is triggered (13 WF CSP PSS Request).<br>20. The registration package is returned from PSSD and the PSS results are reviewed.<br>21. If there are issues with the PSS results, the registration package is returned to PSSD, go to step 18.<br>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.<br>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.<br>24. If there is nothing preventing the organization termination, as required all PSS clearances are terminated.<br>25. The CSP registration analyst notifies the organization's company security officer (CSO) and the organization's sponsor of the termination.<br>26. The registration request is closed-out for non-compliance. Go to step 34.<br>27. CSP registration analyst updates the organization information.<br>28. The file is submitted to the CSP quality assurance officer for review.<br>29. CSP quality assurance officer reviews the file.<br>30. If the CSP quality assurance officer determines modifications are required, the registration request is sent back to the CSP registration analyst for updates.<br>31. CSP registration analyst updates the file, go to step 28.<br>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.<br>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.<br>34. The process ends. |
| Inputs | • Update information<br>• PSSD results |
| Outputs | • Termination notice<br>• Granting letter |

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

| | |
|---|---|
| | 12. CSP registration analyst terminates any PSS requests.<br>13. CSP registration analyst notifies the CSO and sponsor of termination.<br>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<br>• CSP Inspector<br>• CSP Senior Inspector<br>• CSP Inspection Manager<br>• CSP Registration/Contracts |
| Business Objective | • Conduct physical and information technology security reviews of an organization to assess and ensure:<br>○ Organizations are compliant to industrial security requirements.<br>○ Information technology security requirements are met.<br>○ Level of DSC is appropriate.<br>○ Alignment of company and contract information to ensure that all information meets established quality standards.<br>○ Provide advice and guidance to CSO’s on security requirements. |
| Trigger | • Various triggers from other workflows. |
| Workflow Description | 1. Start of process.<br>2. Registration workflow (3 WF CSP Registration New/Upgrade).<br>3. Contract post award workflow (2 WF CSP Contracts Post Award).<br>4. DCS Renewal workflow (6 WF CSP Registration DSC).<br>5. The Senior Inspector review the inspection request.<br>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.<br>29. Decision. Has client provided the DSC information within the 30 day delay? [Yes: Step 29, No: 45].<br>30. Decision. Does the inspector recommend to conduct the inspection onsite instead of offsite? [Yes: Step 30, No: 32]<br>31. The Senior Inspector approves the inspector's recommendation to conduct an onsite inspection instead.<br>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.<br>33. The inspector gathers all the information provide for this inspection.<br>34. The inspector prepares for the inspection.<br>35. The inspector schedules the inspection.<br>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.<br>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.<br>38. The Senior Inspector reviews the report and makes changes, if required. This may include changes to the recommendation(s).<br>39. The Manager will review and sign off the report/recommendation(s).<br>40. Decision. Is Organization Compliant? [Yes: Step 40, No: Step 42]<br>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.<br>42. The inspector closes the inspection request.<br>43. End of Process<br>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.<br>45. Initiate the Inspection Non-Compliant process. (11 WF CSP Inspection Non-Compliant).<br>46. Decision. Is the organization compliant? [Yes: Step 40, No: Step 41]<br>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.<br>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<br>• Approval Letter<br>• Letter/notification to inform organization that did not obtaining the DSC clearance requested<br>• 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<br>• CSP Inspector |
| Business Objective | • Conduct physical and information technology security reviews of an organization to assess and ensure:<br>○ Organizations are compliant to industrial security requirements.<br>○ Information technology security requirements are met.<br>○ Level of DSC is appropriate.<br>○ Alignment of company and contract information to ensure that all information meets established quality standards.<br>○ 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<br>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.<br>3. Decision. Have the recommendations been implemented in the prescribe 30 day delay? [Yes: Step 4, No: Step 7]<br>4. The Inspector conducts the follow-up inspection. This could be an onsite or offsite inspection.<br>5. Decision. Did the inspection pass? [Yes: 6, No: 7]<br>6. End Process. Return to Inspection Workflow.<br>7. Decision. Was the inspection for a New DCS Site? [Yes: Step 8, No: Step 9].<br>8. The inspector prepare and sends the notification that the organization site is not obtaining the DSC clearance as requested.<br>9. The inspector places the organization into Non-Compliance status.<br>10. Decision. Is there ongoing contract with this organization at the site in question? [Yes: Step 16, No: Step 11]<br>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.<br>12. Decision. Have the recommendations been implemented in the additional delay? [Yes: Step 13, No: 15].<br>13. The Inspector conducts the follow-up inspection. This could be an onsite or offsite inspection.<br>14. Decision. Did the inspection pass? [Yes: 6, No: 15]<br>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.<br>16. Initiate the DP 123 process. This is the Compliance and Enforcement with Industrial Security Requirements.<br>17. End process. |
| Inputs | • N/A |

| | |
|---|---|
| Outputs | • Letter/notification to inform organization that did not obtaining the DSC clearance requested.<br>• 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)<br>• CSP Senior Inspector (Senior FISO)<br>• CSP Inspection Manager (FISO Manager)<br>• CISD Director |
| Business Objective | • Conduct investigations where required. |
| Trigger | • Various triggers from the other registration workflows. |
| Workflow Description | 1. Start Process.<br>2. CSP senior inspector performs a preliminary review of the allegation or investigation request.<br>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.<br>4. If the investigation is under the IID mandate, the CSP senior inspector performs a risk assessment and prioritizes the investigation request.<br>5. CSP investigation manager reviews the risk assessment.<br>6. CSP senior inspector assigns the investigation to an inspector based on the investigations risk and the inspector's experience.<br>7. CSP inspector gathers additional information and prepares for the investigation.<br>8. CSP inspector conducts preliminary investigation.<br>9. CSP inspector determines if the investigation is required. If no investigation is required, go to step 39.<br>10. If the investigation is required, the CSP inspector will contact the organization's CSO informing of the investigation.<br>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.<br>13. If the investigation was not classified as high risk from step 4, go to step 15.<br>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.<br>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.<br>16. CSP inspector performs analysis of the investigations findings and determines corrective measures.<br>17. CSP inspector creates a report with corrective recommendations.<br>18. CSP senior inspector or CSP inspection manager reviews the report and recommendations.<br>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.<br>20. If there is a requirement for a warning letter or there will be media coverage, the CISD director reviews the report and recommendations.<br>21. CSP inspector notifies the other divisions if required.<br>22. CSP inspector determines if the allegations are confirmed. If the allegations are not confirmed, go to step 37.<br>23. If the allegations are confirmed, the CSP inspector reports any suspected criminal activity to police authorities.<br>24. CSP inspector notifies the contract authority and prime contractor.<br>25. If the report outlined corrective measures, go to step 26. If there were no corrective measures go to step 35.<br>26. CSP inspector starts the DP 123 process.<br>27. As a result of the DP 123 process, the CSP inspector determines if there is need for immediate revocation.<br>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.<br>29. The revocation letter is signed by the director and sent.<br>30. CSP inspector determines if there is an impact on the organization's employees. If there is no impact, go to step 32.<br>31. If there is an impact on the organization's employees the SSIU process is triggered (22 WF CSP SSIU).<br>32. CSP inspector terminates the organization.<br>33. CSP inspector continues the DP 123 process, go to step 42.<br>34. If the investigation does not fall under the IID mandate, the CSP senior inspector or CSP inspector will prepare a report.<br>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.<br>36. If there is a requirement, a follow-up is scheduled.<br>37. CSP inspector conducts the follow-up. Go to step 42.<br>38. If no allegations were confirmed, the CSP inspector prepares a report.<br>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.<br>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.<br>42. CSP senior inspector closes the investigation.<br>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<br>• Individual (Applicant)<br>• CSP Registration<br>• CSP Screening Specialist |
| Business Objective | • Receipt of and triage of personnel security screening requests. |
| Trigger | • Organization submission of personnel security screening request.<br>• CSP organization registration.<br>• CSP PSSD created personnel security clearance request. |

| | |
|---|---|
| Workflow Description | 1. Start of process.<br>2. Organization’s security official creates a personnel security screening request for an individual employed by the organization.<br>3. Applicant completes the security screening request.<br>4. Organization’s security officer submits the security screening request.<br>5. As part of the organization’s registration with the CSP, a PSS clearance package is created.<br>6. The CSP registration PSS package is transferred to the CSP Personnel Security Screening Division (PSSD).<br>7. In some cases the CSP PSSD have to create personnel security clearance requests.<br>8. CSP PSSD creates personnel security clearance requests based on external requests received by mail, fax or email.<br>9. CSP screening specialist reviews if the request is a termination request. If it is a termination request, go to step 29.<br>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.<br>11. If there are no issues with the request information, go to step 14.<br>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.<br>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.<br>14. If the request received and requires manual input into the PSSD business system, the CSP screening specialist performs the data entry.<br>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.<br>16. The new personnel security process is triggered. (14 WF CSP PSS New).<br>17. If the request is an update to an existing clearance.<br>18. The update personnel security process is triggered. (15 WF CSP PSS Update).<br>19. If the request is an upgrade to an existing clearance.<br>20. The upgrade personnel security process is triggered. (16 WF CSP PSS Upgrade).<br>21. If the request is to transfer a clearance from one organization to another.<br>22. The transfer personnel security process is triggered. (17 WF CSP PSS Transfer).<br>23. If the request is to duplicate an existing clearance.<br>24. The duplicate personnel security process is triggered. (18 WF CSP PSS Duplicate).<br>25. If the request is a reactivate a clearance.<br>26. The reactivation personnel security process is triggered. (19 WF CSP PSS Re-Activation).<br>27. If the request is for a NATO/COSMIC clearance.<br>28. The NATO/COSMIC personnel security process is triggered. (21 WF CSP NATO).<br>29. The termination process is triggered (20 WF CSP PSS Terminate).<br>30. End Process. |

| | |
|---|---|
| Inputs | • Personnel Security Clearance Requests |
| Outputs | • Close-out of security clearance request.<br>• 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.<br>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.<br>3. PSS screening specialist will perform a Credit Check of the individual.<br>4. PSS screening specialist will determine if an Out of Country Verification (OCC) is required. If no OCC is required, go to step 6.<br>5. If an OCC is required, an OCC is performed.<br>6. PSS screening specialist analyzes the results from the fingerprints, credit and OCC checks.<br>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.<br>8. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 11.<br>9. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>10. If no additional processing is required, go to step 50.<br>11. If the request requires reliability enhanced status, continue, otherwise go to step 20.<br>12. For reliability enhanced status, the PSS screening specialist will trigger the following security checks, Law Enforcement Record Check (LERC).<br>13. PSS screening specialist will request that the individual completed a security questionnaire or partake in a security interview.<br>14. PSS screening specialist will perform an open source inquiry of the individual.<br>15. PSS screening specialist analyzes the results from the LERC, security questionnaire/interview and open source inquiry.<br>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.<br>17. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 20.<br>18. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>19. If no additional processing is required, go to step 50.<br>20. If the request requires secret and site access clearance, continue, otherwise go to step 27.<br>21. For secret and site access clearance, the PSS screening specialist will trigger a CSIS security assessment.<br>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.<br>24. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 27.<br>25. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>26. If no additional processing is required, go to step 50.<br>27. If the request requires a top secret clearance, continue, otherwise go to step 34.<br>28. For a top secret clearance, the PSS screening specialist will trigger a CSIS security assessment.<br>29. PSS screening specialist analyzes the results from the CSIS security assessment.<br>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.<br>31. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 34.<br>32. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>33. If no additional processing is required, go to step 50.<br>34. If the request requires a top secret SIGNIT clearance, continue, otherwise go to step 39.<br>35. For top secret SIGNIT clearance, the PSS screening specialist will trigger an additional credit check.<br>36. The PSS screening specialist will then trigger a SSIU subject interview.<br>37. The SSIU process is triggered (22 WF CSP PSS SSIU).<br>38. If no additional processing is required, go to step 50.<br>39. If the top secret enhance clearance is required, continue, otherwise go to step 48.<br>40. For top secret enhance clearance, the PSS screening specialist will trigger a security questionnaire or interview.<br>41. PSS screening specialist will perform an open source inquiry.<br>42. PSS screening specialist will request a CSIS security assessment.<br>43. PSS screening specialist will request the individual undergo a polygraph examination.<br>44. PSS screening specialist analyzes the results from the security questionnaire/interview, open source inquiry, CSIS security assessment and polygraph results.<br>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.<br>46. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 48.<br>47. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). Go to step 50.<br>48. PSS screening specialist performs a completeness verification on the personnel security request.<br>49. PSS screening specialist creates the briefing certificate and sends it to the organizations CSO.<br>50. Return to the PSS Requests process to end (13 WF CSP PSS Request). |
| Inputs | • Personnel Security Clearance Request<br>• Results from the various security checks (credit checks, CSIS security assessment, etc.) |
| Outputs | • Granting of personnel security clearance request<br>• 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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>7. CSP security specialist will update the individual’s information based on the provided information.<br>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.<br>9. If there was no change in personal circumstance, the CSP security specialist notifies CSIS.<br>10. CSP security specialist will contact CSIS with the new information and request a new CSIS security assessment.<br>11. CSP security specialist analyzes the results of the CSIS security assessment. If there were no adverse results, go to step 13.<br>12. If the CSIS security assessment produced adverse results the SSIU process (22 WF CSP PSS SSIU) is triggered. Go to step 15.<br>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.<br>15. Return to the PSS Requests process to end (13 WF CSP PSS Request). |
| Inputs | • Personnel Security Clearance Request<br>• 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.<br>2. If the request is to upgrade to a reliability enhanced status, continue, otherwise go to step 16.<br>3. PSS screening specialist will assess the request to determine if the reliability security checks need to be redone.<br>4. If there is no need to redo the reliability security checks, go to step 8.<br>5. PSS screening specialist analyzes the results from the reliability security checks. If there were no adverse results, go to step 7.<br>6. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU).<br>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).<br>9. PSS screening specialist will request that the individual completed a security questionnaire or partake in a security interview.<br>10. PSS screening specialist will perform an open source inquiry of the individual.<br>11. PSS screening specialist analyzes the results from the LERC, security questionnaire/interview and open source inquiry.<br>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.<br>13. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 15.<br>14. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>15. If no additional processing is required, go to step 64.<br>16. If the request is to upgrade to secret and site access clearance, continue, otherwise go to step 28.<br>17. PSS screening specialist will assess the request to determine if the secret security checks need to be redone.<br>18. If there is no need to redo the secret security checks, go to step 22.<br>19. PSS screening specialist analyzes the results from the secret security checks. If there were no adverse results, go to step 21.<br>20. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU).<br>21. If no additional processing is required, go to step 66.<br>22. For secret and site access clearance, the PSS screening specialist will trigger a CSIS security assessment.<br>23. PSS screening specialist analyzes the results from the CSIS security assessment.<br>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.<br>25. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 27.<br>26. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>27. If no additional processing is required, go to step 64.<br>28. If the request is to upgrade to top secret clearance, continue, otherwise go to step 40.<br>29. PSS screening specialist will assess the request to determine if the top secret security checks need to be redone.<br>30. If there is no need to redo the top secret security checks, go to step 34.<br>31. PSS screening specialist analyzes the results from the top secret security checks. If there were no adverse results, go to step 33.<br>32. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU).<br>33. If no additional processing is required, go to step 66.<br>34. For a top secret clearance, the PSS screening specialist will trigger a CSIS security assessment.<br>35. PSS screening specialist analyzes the results from the CSIS security assessment.<br>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.<br>37. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 39.<br>38. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU).<br>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.<br>41. PSS screening specialist will assess the request to determine if the top secret SIGNIT security checks need to be redone.<br>42. If there is no need to redo the top secret SIGNIT security checks, go to step 46.<br>43. PSS screening specialist analyzes the results from the top secret SIGNIT security checks. If there were no adverse results, go to step 45.<br>44. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU).<br>45. If no additional processing is required, go to step 66.<br>46. For top secret SIGNIT clearance, the PSS screening specialist will trigger an additional credit check.<br>47. The PSS screening specialist will then trigger a SSIU subject interview.<br>48. The SSIU process is triggered (22 WF CSP PSS SSIU).<br>49. If no additional processing is required, go to step 64.<br>50. The request is to upgrade to top secret enhanced clearance.<br>51. PSS screening specialist will assess the request to determine if the top secret security checks need to be redone.<br>52. If there is no need to redo the top secret security checks, go to step 56.<br>53. PSS screening specialist analyzes the results from the top secret security checks. If there were no adverse results, go to step 55.<br>54. If there were adverse results, trigger the SSIU process (22 WF CSP PSS SSIU).<br>55. If no additional processing is required, go to step 66.<br>56. For top secret enhance clearance, the PSS screening specialist will trigger a security questionnaire or interview.<br>57. PSS screening specialist will perform an open source inquiry.<br>58. PSS screening specialist will request a CSIS security assessment.<br>59. PSS screening specialist will request the individual undergo a polygraph examination.<br>60. PSS screening specialist analyzes the results from the security questionnaire/interview, open source inquiry, CSIS security assessment and polygraph results.<br>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.<br>62. PSS screening specialist determines if they should apply the risk matrix. If the matrix is to be applied, go to step 64.<br>63. If the matrix is not applicable, trigger the SSIU process (22 WF CSP PSS SSIU). Go to step 66.<br>64. PSS screening specialist performs a completeness verification on the personnel security request.<br>65. PSS screening specialist creates the briefing certificate and sends it to the organizations CSO.<br>66. Return to the PSS Requests process to end (13 WF CSP PSS Request). |
| Inputs | • Personnel Security Clearance Request<br>• Results from the various security checks (credit checks, CSIS security assessment, etc.) |
| Outputs | • Granting of personnel security clearance request<br>• 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.<br>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.<br>3. Verify that the existing clearance is still active.<br>4. If the clearance is not valid, continue, otherwise go to step 7.<br>5. Notify the OGD of invalid clearance and inability to transfer file<br>6. Close out request, go to step 23.<br>7. If the clearance requires no renewal, continue, otherwise go to step 9<br>8. Attach a note on the file to the OGD stating a renewal is required.<br>9. Send a copy of clearance to the requesting OGD.<br>10. Notify CSIS of the transfer of the request, go to step 23.<br>11. If OGD states the clearance is not valid, continue, otherwise go to step 14<br>12. Close out transfer request.<br>13. Notify CSO of the new to submit a new request as the transfer request cannot be completed. Go to step 23.<br>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.<br>16. Continue with the transfer at the level of applicant's clearance/status.<br>17. Assess the request to determine if security checks need to be redone.<br>18. If security checks must be redone, continue, otherwise go to step 21.<br>19. If adverse results are found when redoing security checks, continue, otherwise go to step 21.<br>20. Trigger the SSIU process (22 WF CSP PSS SSIU).<br>21. Verify completeness of the request.<br>22. Create a briefing certificate for the request and send it to the CSO.<br>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.<br>2. If no valid personnel security clearance exists at the level requested, continue, otherwise go to step 5.<br>3. Close out request.<br>4. Notify CSO of the need to submit a new screening request as the previous level requested cannot be duplicated. Go to step 11.<br>5. Assess the previous request to determine if additional security checks need to be redone.<br>6. If security checks must be redone, continue, otherwise go to step 9.<br>7. If adverse results are found when redoing security checks, continue, otherwise go to step 9.<br>8. Trigger the SSIU process (22 WF CSP PSS SSIU).<br>9. Verify completeness of the request.<br>10. Create a briefing certificate for the request and send it to the CSO.<br>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.<br>2. If the clearance to be re-activated has been terminated for over 2 years, continue, otherwise go to step 5.<br>3. Close out re-activation request.<br>4. Notify CSO of the need to submit a new screening request. Go to step 14.<br>5. If the clearance to be re-activated has been terminated between 1 and 2 years, continue, otherwise go to step 9.<br>6. Redo necessary security checks.<br>7. If adverse results are found when redoing security checks, continue, otherwise go to step 11.<br>8. Trigger the SSIU process (22 WF CSP PSS SSIU).<br>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.<br>10. No termination has ever been received and the initial request is still active<br>11. Duplicate the clearance request.<br>12. Verify completeness of the request.<br>13. Create a briefing certificate for the request and send it to the CSO.<br>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<br>• Personnel Screening Specialist |
| Business Objective | • To terminate a personnel security clearance. |
| Trigger | • Personnel screening termination requirement. |

| | |
|---|---|
| Workflow Description | 1. Start of process.<br>2. Organization’s Security Official submits a request to terminate a PSS request. If the request is submitted through OLISS, go to step 6.<br>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.<br>4. If the signature is not on the termination request, the screening specialist requests a signed termination form from the CSO.<br>5. If the information is not received, the screening specialist will close-out the request.<br>6. If the CSO submits an OLISS request to terminate a PSS, the request is matched to the existing Personnel ID.<br>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.<br>8. If a PSS request for the same organization is still pending with CSIS, the screening specialist will notify CSIS of the termination request.<br>9. The screening specialist terminates the PSS request.<br>10. The PSS request is set to “Struck off Strength”.<br>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<br>• NATO Partner<br>• 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.<br>2. CSO submits a NATO clearance request.<br>3. NATO request initiated by PSSD.<br>4. The screening specialist verifies if there is an existing and valid clearance for the individual (including DC Pending NATO requests).<br>5. If there is no valid clearance, the screening specialist will initiate a security clearance request.<br>6. The screening specialist will identify the type/level of security clearance required and follow the PSSD process.<br>7. If there is a valid clearance, the screening specialist will assign the NATO request to the Pending NATO Workflow for IISD to action.<br>8. The IISD analyst will first verify if a National Clearance is granted. If a clearance has not been granted, return to step 5.<br>9. If the National Clearance is granted, the IISD analyst will verify if the individual is a Canadian Citizen.<br>10. If the individual is a Canadian Citizen, the IISD analyst will determine if the NATO FSC meets or exceed the requirements level.<br>11. If the individual is not a Canadian Citizen, the ISSD analyst will verify if the individual is a NATO National.<br>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.<br>13. The IISD Analyst performs the Personnel Security Clearance Information sheet process.<br>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.<br>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.<br>16. If the approval is valid, the IISD analyst will complete the NATO letter process.<br>17. The IISD analyst will inform the organization of the assessment results.<br>18. The IISD analyst will send a briefing form to the CSO for signature.<br>19. The CSO must return the signed briefing form to IISD within 10 working days.<br>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<br>21. The signed briefing form is received by IISD within 10 working days.<br>22. The IISD analyst reviews the signed briefing form.<br>23. The IISD analyst will match the NATO expiry date to the National Clearance expiry date.<br>24. The IISD Analyst will determine if the NATO request is granted or denied.<br>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.<br>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.<br>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<br>• Personnel Screening Specialist<br>• Security Screening Investigation Unit (SSIU) Team<br>• CISD Director<br>• PWGSC Legal Team<br>• 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.<br>2. Inspections/Investigations Division submits a request or provides information to SSIU (10 WF CSP Inspections or 12 WF CSP Investigations).<br>3. PSSD receives a request requiring an SSIU investigation.<br>4. PSSD submits a request or provides information to SSIU.<br>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.<br>7. If the file is not missing any information and the checks have been verified, a CSIS assessment must be completed when required.<br>8. The SSUI Liaison Officer transfers the file to the SSIU Chief for triage.<br>9. The SSIU Chief will determine if the PSS will be suspended.<br>10. The SSIU Chief determines the PSS is to be suspended based on the security request type of the file.<br>11. If the security request is at the classified level, the file will be sent to the Deputy Minister for suspension approval.<br>12. If the security request is at the reliability level, the file will be sent to the CISD Director for suspension approval.<br>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.<br>14. If an SSIU investigation is required, the SSIU Chief assigns the file to an SSIU Officer for action.<br>15. The SSIU Officer prepares for a resolution of doubt interview with the individual.<br>16. The SSIU Officer conducts a resolution of doubt interview with the individual.<br>17. Following the interview, the SSIU Officer will verify and validate the resolution of doubt interview results.<br>18. The SSIU Officer will complete an SSIU report and propose a recommendation for the file.<br>19. If the recommendation from the SSIU Officer is a denial of the PSS, a denial package is prepared by the officer.<br>20. The SSIU officer must determine if a follow-up interview is required with the individual.<br>21. If a follow-up interview is required, the SSIU Officer will schedule an interview with the individual.<br>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.<br>23. The SSIU Chief will review the report and recommendation.<br>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.<br>25. If a follow-up interview is not required, the SSIU Chief will determine is modifications are required for the report and recommendation proposed.<br>26. If the SSIU chief determines modifications are required, the SSIU Officer will update the report and recommendation. Once updated, go to step 22.<br>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.<br>28. If the recommendation is to grant the PSS request, go to step 29.<br>29. The SSIU Liaison Officer grants the PSS request.<br>30. The SSIU Liaison Officer verifies if any additional processing is required. If there is no additional processing required, go to step 50.<br>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.<br>32. If the recommendation is to close out the PSS request, go to step 33.<br>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.<br>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.<br>36. If the recommendation is to deny or revoke the PSS request, go to step 37.<br>37. The report and denial letter is reviewed by the legal team.<br>38. If the legal team determines that no modifications are required for the report and/or the denial letter, go to step 40.<br>39. The SSIU Chief must update the report and denial letter proposed by the legal team. Once completed, go to step 37.<br>40. The report and denial letter will be reviewed once again by the legal team for final approval.<br>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.<br>42. If the CISD director determines that modifications are required for the report and/or denial letter, go to step 43.<br>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.<br>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.<br>45. If the security request type of the file is at the classified level, the Deputy Minister must review the report and denial letter.<br>46. If the Deputy Minister determines that modifications are required for the report and/or denial letter, go to step 47.<br>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.<br>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.<br>49. The SSIU Liaison Officer will send a notification to the CSO, the Individual and CSIS of the decision.<br>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.)<br>• Call Centre Analyst<br>• Call Centre Senior Analyst<br>• 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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>9. Call Center Senior Analyst triages the inquiry to determine which ISP business line to transfer the request to.<br>10. Call Center Senior Analyst sends the inquiry to the ISP business line for response. Continue at step 12.<br>11. Call Center Senior Analyst in conjunction with the Call Center Analyst develops the inquiry response. Go to step 14.<br>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.<br>13. Call Center Analyst develops the inquiry response.<br>14. Call Center Analyst provides the inquiry response to the client.<br>15. Call Center Analyst logs the call within the business system DISIS for tracking purposes.<br>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<br>• 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<br>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:<br>a. Canada to Canada, Canada to United States and Canada to Foreign visit requests are received via email.<br>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.<br>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.<br>3. CSP Visit Officer reviews the RFV.<br>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.<br>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.<br>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.<br>7. CSP Visit Officer sends a request to the RFV security officer for missing information.<br>8. Security Official provides the required information. Go to step 3.<br>9. RFV type is a Canada to Canada visit.<br>10. Canada to Canada visit is either of subtype Industry or DND. If DND go to step 13, otherwise go to step 11.<br>11. CSP Visit Officer requests host site concurrence for the visit.<br>12. CSP Visit Officer receives host site response for concurrence. Go to step 24.<br>13. CSP Visit Officer sends the RFV to DND. Go to step 24.<br>14. DND approves the RFV and notifies the CSP. Go to step 24.<br>15. RFV type is a United States to Canada visit. Go to step 17.<br>16. RFV type is a Foreign to Canada visit.<br>17. CSP Visit Officer requests host site concurrence for the visit.<br>18. CSP Visit Officer receives host site response for concurrence. Go to step 24.<br>19. RFV type is Canada to Foreign visit. Go to step 21.<br>20. RFV type is Canada to United States visit.<br>21. CSP Visit Officer requests foreign DSO concurrence.<br>22. CSP Visit Officer received foreign DSO concurrence.<br>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.<br>24. CSP Visit Officer creates the RFV approval notice. Go to step 26.<br>25. CSP Visit Officer creates the RFV rejection notice.<br>26. CSP Visit Officer sends the notification to the security official who submitted the RFV and the visit's host site.<br>27. The process ends. |
| Inputs | • Request for Visit<br>• Contract security clauses<br>• Host site concurrence |
| Outputs | • Request for visit approval or rejection<br>• 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)<br>• CGP Program Support Clerk<br>• CGP Program Support Information Officer<br>• CGP Registration Coordinator<br>• CGP Registration Chief<br>• CGP Registration Analyst<br>• CGP Operations Manager<br>• CGP Case Management and Best Practices (CMBP)<br>• CGP Investigations and Analysis Unit (IAU)<br>• CGP Program Management and Learning (PML)<br>• 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.<br>2. Applicant completes and submits the CGP registration application.<br>3. CGP program support clerk reviews the registration application.<br>4. CGP program support clerk determine if all required information has been received. If all information received, go to step 7.<br>5. If there is missing information, CGP program support clerk requests missing information from applicant.<br>6. Applicant provides requested information, go to step 2.<br>7. CGP program support clerk performs preliminary data entry.<br>8. CGP program support information officer validates the application.<br>9. CGP program support information officer determines if all required information has been received. If all information has been received, go to step 14.<br>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.<br>12. Applicant provides the missing information. Go to step 8.<br>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.<br>14. If all the information was received, CGP program support clerk completes the data entry of the application.<br>15. CGP program support information performs a QC of the inputted data.<br>16. CGP program support information reviews the applicant's security assessment (SAA) as part of the application.<br>17. CGP program support information notifies the applicant that the CGP registration is in process.<br>18. CGP program support information requests security checks (Fingerprints, Criminal Record Name Check, Credit Check, etc.) as required.<br>19. CGP program support information notifies PML if an organization's Designated Official (DO) requires training.<br>20. CGP training process is triggered. (28 WF CGP Designated Official Training).<br>21. CGP registration coordinator triages and assigns the registration application to a CGP registration analyst for processing.<br>22. CGP registration analyst reviews the application and SAA for completeness.<br>23. CGP registration analyst determines if all required information has been received. If all the required information has been received, go to step 26.<br>24. CGP registration analyst requests the missing information from the applicant.<br>25. Applicant provides the missing information. Go to step 22.<br>26. CGP registration analyst completes the registration data entry.<br>27. CGP registration analyst analyzes the application and SAA.<br>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.<br>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.<br>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.<br>31. If a CGP CMBP referral is required, the CGP CMBP process is triggered (34 WF CGP CMBP). Go to step 32.<br>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.<br>33. If the CGP registration application is considered to be high risk, the CGP registration analyst creates an escalation request.<br>34. CGP operations manager triages the escalation request and makes a determination to reject or approve the CGP registration application. Go to step 32.<br>35. If the CGP registration application is rejected, CGP registration analyst creates a rejection report.<br>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.<br>38. If the CGP registration application is approved, CGP registration analyst creates an approval report.<br>39. CGP registration chief QC's the approval report.<br>40. If the approval report's QC fails, the CGP registration analyst is required to make amendments, go to step 38.<br>41. If the approval report's QC passes, the CGP registration chief performs some minor data entry.<br>42. CGP registration chief activates the organization's sites within the CGP business system.<br>43. CGP registration chief approves the organization and required individual SAA's.<br>44. CGP registration analyst finalizes the data entry.<br>45. CGP registration analyst creates an inspection request, which triggers the CGP inspection workflow.<br>46. CGP Inspection workflow is triggered (30 WF CGP Inspections).<br>47. CGP registration analyst creates and sends to organization registration correspondence package.<br>48. Process ends. |
| Inputs | • Organization's registration application<br>• Individuals security assessment applications<br>• Security checks |
| Outputs | • Approval or rejection of CGP registration application<br>• CGP registration package<br>• 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)<br>• CGP Program Support Clerk<br>• CGP Program Support Information Officer<br>• CGP Registration Coordinator<br>• CGP Investigations and Analysis Unit (IAU)<br>• CGP Program Management and Learning (PML)<br>• CGP Compliance |
| Business Objective | • To apply amendments to an organizations CGP registered information. Can be one of the following types of amendments:<br>○ Organization termination request<br>○ Amendment to CGP information<br>○ Submission of a security assessment |

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

| | |
|---|---|
| Workflow Description | 1. Start of process<br>2. Applicant submits amendment request to CGP.<br>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.<br>4. CGP program support applies the amendment. Go to step 28.<br>5. If the amendment is a request for a temporary worker exemption, go to step 4, otherwise go to step 7.<br>6. The CGP IAU temporary workers exemption process is triggered (31 WF CGP Temp Worker Exemption).<br>7. CGP registration coordinator receives the amendment and reviews the amendment information. If the amendment information is complete go to step 9.<br>8. If the amendment information is deemed incomplete by the CGP registration coordinator, request information from applicant.<br>9. Applicant provides the requested information, go to step 1.<br>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.<br>11. If the CGP registration coordinator determines it is an information only amendment, go to the next step, otherwise go to step 15.<br>12. The CGP registration coordinator will apply the information amendment.<br>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.<br>14. The CGP inspection process is triggered (30 WF CGP Inspections).<br>15. If the CGP registration coordinator determines it is an organization termination request.<br>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.<br>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.<br>18. If the CGP registration coordinator determines a security assessment is required, continue to next step, otherwise go to step 21.<br>19. The CGP registration coordinator conducts a security assessment.<br>20. CGP registration coordinator applies the security assessment information to the organization.<br>21. After the CGP registration coordinator performs the security assessment, if training is not required, go to step 23.<br>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).<br>23. If the CGP registration coordinator determines the amendment requires a business assessment, continue to the next step, otherwise go to step 25.<br>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.<br>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.<br>27. CGP registration coordinator applies the business assessment amendment.<br>28. Process ends. |
| Inputs | • Submitted amendment |
| Outputs | • Processed amendment<br>• 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)<br>• CGP Program Support Clerk<br>• CGP Program Support Information Officer<br>• CGP Registration Coordinator<br>• CGP Registration Chief<br>• CGP Registration Analyst<br>• CGP Operations Manager<br>• CGP Case Management and Best Practices (CMBP)<br>• CGP Investigations and Analysis Unit (IAU)<br>• CGP Program Management and Learning (PML)<br>• 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.<br>2. CGP program support clerk creates a list of CGP registered organizations that are expiring and notifies the organization of their renewal requirements.<br>3. Applicant completes and submits the CGP registration application. |

| | |
|---|---|
| | 4. CGP program support clerk reviews the registration application.<br>5. CGP program support clerk determine if all required information has been received. If all information received, go to step 7.<br>6. If there is missing information, CGP program support clerk requests missing information from applicant.<br>7. Applicant provides requested information, go to step 3.<br>8. CGP program support clerk performs preliminary data entry.<br>9. CGP program support information officer validates the application.<br>10. CGP program support information officer determines if all required information has been received. If all information has been received, go to step 15.<br>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.<br>12. If the application is not being rejected, the CGP program support information officer requests the missing information from the applicant.<br>13. Applicant provides the missing information. Go to step 9.<br>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.<br>15. If all the information was received, CGP program support clerk completes the data entry of the application.<br>16. CGP program support information performs a QC of the inputted data.<br>17. CGP program support information reviews the applicant’s security assessment (SAA) as part of the application.<br>18. CGP program support information notifies the applicant that the CGP registration is in process.<br>19. CGP program support information requests security checks (Fingerprints, Criminal Record Name Check, Credit Check, etc.) as required.<br>20. CGP program support information notifies PML if an organization’s Designated Official (DO) requires training.<br>21. CGP training process is triggered. (28 WF CGP Designated Official Training).<br>22. CGP registration coordinator triages and assigns the registration application to a CGP registration analyst for processing.<br>23. CGP registration analyst reviews the application and SAA for completeness.<br>24. CGP registration analyst determines if all required information has been received. If all the required information has been received, go to step 27.<br>25. CGP registration analyst requests the missing information from the applicant.<br>26. Applicant provides the missing information. Go to step 23.<br>27. CGP registration analyst completes the registration data entry.<br>28. CGP registration analyst analyzes the application and SAA.<br>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.<br>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.<br>32. If a CGP CMBP referral is required, the CGP CMBP process is triggered (34 WF CGP CMBP). Go to step 33.<br>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.<br>34. If the CGP registration application is considered to be high risk, the CGP registration analyst creates an escalation request.<br>35. CGP operations manager triages the escalation request and makes a determination to reject or approve the CGP registration application. Go to step 33.<br>36. If the CGP registration application is rejected, CGP registration analyst creates a rejection report.<br>37. CGP registration chief QC's the rejection report.<br>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.<br>39. If the CGP registration application is approved, CGP registration analyst creates an approval report.<br>40. CGP registration chief QC's the approval report.<br>41. If the approval report's QC fails, the CGP registration analyst is required to make amendments, go to step 39.<br>42. If the approval report's QC passes, the CGP registration chief performs some minor data entry.<br>43. CGP registration chief activates the organization's sites within the CGP business system.<br>44. CGP registration chief approves the organization and required individual SAA's.<br>45. CGP registration analyst finalizes the data entry.<br>46. CGP registration analyst creates an inspection request, which triggers the CGP inspection workflow.<br>47. CGP Inspection workflow is triggered (30 WF CGP Inspections).<br>48. CGP registration analyst creates and sends to organization registration correspondence package.<br>49. Process ends. |
| Inputs | • Organization's registration renewal application<br>• Individuals security assessment applications<br>• Security checks<br>• Other supporting documentation |
| Outputs | • Approval or rejection of CGP registration application<br>• CGP registration package<br>• 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)<br>• CGP Program Support Information Officer<br>• 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.<br>1. CGP PML received notification that an individual requires the DO training.<br>2. CGP PML sends notification to trainee, requesting the trainee to register for the Designated Official Certification Program (DOCP) course.<br>3. Trainee completes course registration.<br>4. Trainee has 30 days to register for the course.<br>5. CGP PML receives all DOCP course registrations.<br>6. CGP PML records course registration information.<br>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.<br>8. CGP PML records the validated course registration.<br>9. CGP PML sends instructions to the trainee on how to retrieve the course package prior to taking training.<br>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.<br>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.<br>12. Trainee takes the DOCP training.<br>13. Trainee takes the DOCP exam.<br>14. CGP PML grades the exam.<br>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.<br>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.<br>18. CGP PML reject the course registration.<br>19. CGP PML sends notification to individual that they are not eligible to take the DOCP training.<br>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.<br>21. Trainee decides to take the exam.<br>22. Trainee registers for exam only.<br>23. Trainee notifies CGP PML of decision to retake the exam.<br>24. Trainee decides to redo the training, go to step 2.<br>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.<br>26. Trainee decides to not attend course, sends notification to CGP PML to cancel their existing course registration.<br>27. CGP PML cancels trainee registration.<br>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.<br>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<br>• CGP Inspector<br>• CGP Case Management and Best Practices (CMBP)<br>• CGP Investigations and Analysis Unit (IAU) Analyst<br>• 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.<br>1. CGP registration analyst or CGP inspector submits request for cause referral including all supporting documentation.<br>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.<br>3. CGP IAU analyst submits to CGP partner organizations for assessment. CGP partner organizations include RCMP, CSIS, etc.<br>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.<br>5. CGP IAU analyst cancels the “For Cause Referral”, go to step 9.<br>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.<br>7. The CGP CMBP process is triggered (34 WF CGP CMBP).<br>8. CGP IAU forms a recommendation on the referral.<br>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.<br>10. CGP registration or CGP inspection receive the CGP IAU analysts cancellation notice or recommendation notice.<br>11. Process ends. |
| Inputs | • For cause referral request<br>• Justification for referral<br>• CGP partner assessment |
| Outputs | • Request for CGP partner assessment<br>• Referral of for cause referral to CGP CMBP |

### 1.2.6 Inspection

| **Workflow ID** | **30 WF CGP Inspections** |
|---|---|
| Business Unit(s) | • Industry Organization<br>• CGP Registration<br>• CGP Management<br>• CGP Case Management and Best Practices (CMBP)<br>• CGP Investigations and Analysis Unit (IAU)<br>• CGP Compliance Quality Control Officer (QC)<br>• CGP Compliance Inspector (Inspector)<br>• CGP Compliance Travel Coordinator<br>• 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.<br>1. CGP compliance QC will review and categorize received inspection request.<br>2. CGP compliance QC reviews list of unassigned inspection requests sorted by inspection location.<br>3. CGP compliance QC determines if inspection request can be deferred. If the inspection request cannot be deferred, go to step 8.<br>4. CGP compliance QC prepares deferral recommendation.<br>5. CGP compliance inspection manager reviews deferral recommendation.<br>6. If the CGP compliance inspection manager does not approve the deferral recommendation, go to step 8.<br>7. If the CGP compliance inspection manager approves the deferral recommendation, the CGP compliance QC defers the unassigned inspection request. Return to step 2.<br>8. CGP compliance QC reviews inspection team's individual schedules.<br>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.<br>10. CGP compliance QC will repeat this process until there are no unassigned inspection requests, repeat at step 2, otherwise continue.<br>11. CGP compliance QC reviews the list of deferred inspections to identify those that could be used to complete an inspection request block.<br>12. CGP compliance QC will un-defer the inspection request and assign it to a CGP compliance inspector.<br>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.<br>14. CGP compliance inspector reviews assigned inspection request.<br>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.<br>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.<br>17. If the inspection can be completed with a phone inspection, the CGP compliance inspector will contact the organization and conduct the phone inspection.<br>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.<br>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.<br>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).<br>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.<br>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.<br>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.<br>25. CGP compliance travel coordinator approvals the travel itinerary and makes necessary travel arrangements on behalf of the CGP compliance inspector.<br>26. CGP compliance inspector emails the inspection site contact to introduce themselves and arrange a date and time for the inspection.<br>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.<br>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.<br>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.<br>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.<br>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.<br>32. The CGP compliance inspector sends an email to the inspection site contact confirming the date and time that was arranged for the inspection.<br>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.<br>35. CGP compliance inspector requests the registration files from the file room for each registrant in their inspection request block.<br>36. CGP compliance inspector receives the registration files.<br>37. The CGP compliance inspector completes sections 7 to 10 of the pre-inspection checklist for those inspections request within the inspection request block.<br>38. CGP compliance inspector confirms travel approval. If travel approval has not been obtained, seek travel approval.<br>39. CGP compliance inspector conducts the inspection.<br>40. CGP compliance inspector completes the inspection questionnaire.<br>41. CGP compliance inspector completes the compliance inspection form.<br>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.<br>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.<br>44. If the deficiencies were not resolved by the agreed date, go to step 47.<br>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.<br>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.<br>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.<br>48. CGP compliance inspector completes a CMBP report which then triggers the CGP CMBP process (34 WF CGP CMBP).<br>49. CGP compliance QC performs a QC on the inspection report, if QC passes go to step 52.<br>50. If the QC fails, the CGP compliance QC returns the inspection report back to the CGP compliance inspector for corrections.<br>51. CGP compliance inspector updates the inspection report and submits back to QC, go to step 49.<br>52. Process ends. |
| Inputs | • Inspection request from various triggers<br>• Inspection checklist<br>• Inspection questionnaire |
| Outputs | • Registrant is deemed compliant<br>• Inspection has discovered compliance deficiencies that require action<br>• Registrant is deemed non-compliant<br>• CMBP referral<br>• 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)<br>• CGP Investigations and Analysis Unit (IAU) Analyst<br>• CGP Case Management and Best Practices (CMBP)<br>• 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.<br>1. Organization DO submits a temporary worker request package<br>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.<br>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.<br>4. CGP IAU analyst submits a referral to CGP organizational partners for an assessment.<br>5. CGP IAU analyst perms a detailed analysis of the temporary worker request along with the partner assessment.<br>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.<br>7. The CGP CMBP process is triggered (34 WF CGP CMBP).<br>8. CGP IAU analyst approves the temporary worker exemption without conditions, creates the exemption certificate and sends it to the DO.<br>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.<br>10. CGP IAU analyst determines that the temporary worker exemption request is to be denied. The DO is notified of the denial.<br>11. Process ends. |
| Inputs | • CGP application for exemption from registration – Temporary Worker form<br>• Temporary worker security assessment form<br>• Copy of work permit issued by Citizenship and Immigration Canada<br>• Original certificate of good conduct<br>• Copy of a valid passport |

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

### 1.2.8 Visitor Exemptions

| Workflow ID | 32 WF CGP Visitor Exemption |
|---|---|
| Business Unit(s) | • Registering Organization's Designated Official (DO)<br>• CGP Investigations and Analysis Unit (IAU) Analyst<br>• 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.<br>1. Organization DO submits a visitor request package<br>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.<br>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.<br>4. CGP IAU analyst performs a detailed analysis of the visitor request.<br>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).<br>6. CGP IAU analyst approves the visitor exemption without conditions, creates the exemption certificate and sends it to the DO.<br>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.<br>8. CGP IAU analyst determines that the visitor exemption request is to be denied. The DO is notified of the denial.<br>9. Process ends. |
| Inputs | • Visitor application for exemption form<br>• Copy of valid passport<br>• Copy of valid export permit if applicable |

| | |
|---|---|
| Outputs | • CMBP referral<br>• Exemption certificate (with conditions were required) for approved visitors<br>• Letter of exemption<br>• 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)<br>• CGP Investigations and Analysis Unit (IAU) Analyst<br>• CGP Case Management and Best Practices (CMBP)<br>• 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.<br>1. Organization DO submits an industry employee referral request package<br>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.<br>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.<br>4. CGP IAU analyst submits a referral to CGP organizational partners for an assessment.<br>5. CGP IAU analyst perms a detailed analysis of the employee referral request along with the partner assessment.<br>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.<br>7. The CGP CMBP process is triggered (34 WF CGP CMBP).<br>8. CGP IAU analyst confirms the DO’s risk assessment. The CGP IAU analyst creates a referral letter and provides it to the DO.<br>9. CGP IAU analyst modifies the DO’s risk assessment. The CGP IAU analyst creates a referral letter and provides it to the DO.<br>10. Process ends. |

| | |
|---|---|
| Inputs | • Employee security assessment completed by the DO<br>• Original certificate of good conduct<br>• Proof of citizenship<br>• 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<br>• CGP Registration<br>• CGP Management<br>• CGP Case Management and Best Practices (CMBP)<br>• CGP Investigations and Analysis Unit (IAU)<br>• CGP Compliance Quality Control Officer (QC)<br>• CGP Compliance Inspector (Inspector)<br>• Policy Agencies<br>• 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.<br>• CMBP investigations are triggered on an as required basis. |
| Workflow Description | 1. Start of process.<br>2. CMBP referral request submitted to CMBP.<br>3. CMBP Manager reviews and assigns the referral to a Case Management Officer.<br>4. CMBP Case Management Officer creates a case file.<br>5. CMBP Case Management Officer determines if a violation occurred. If there was a violation continue to step 6, otherwise go to step 25.<br>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.<br>8. CMBP Manager prepares a letter of intent outlining the compliant and steps to resolve.<br>9. CMBP Case Management Officer sends letter of intent to registrant.<br>10. If new information regarding the complaint is received continue to step 11, otherwise, if no new information was received go to step 14.<br>11. CMBP Case Management Officer performs analysis of the newly received information.<br>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.<br>13. CMBP Case Management Officer briefs the CGD on the outcome of the complaint. Go to step 25.<br>14. CMBP Manager prepares a recommendation to the Director of the CGP to suspend the registrant.<br>15. CGP Director reviews and assesses the recommendation to suspend.<br>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.<br>17. CMBP Case Management Officer re-instates the registrant or exemption.<br>18. CMBP Case Management Officer notifies the registrant of suspension. Go to step 25.<br>19. CMBP Manager prepares a recommendation to the Director of the CGP to revoke the registrant.<br>20. CGP Director reviews and assesses the recommendation to revoke.<br>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.<br>22. CMBP Case Management Officer notifies the registrant of revocation.<br>23. CMBP Case Management Officer notifies the CGP Inspection of a requirement to perform a Close-Out Inspection activity.<br>24. The CGP Inspection process is triggered (30 WF CGP Inspections).<br>25. CMBP Case Management Officer closes the CMBP case file and creates CMBP report.<br>26. Process ends. |
| Inputs | • CMBP referral request |
| Outputs | • CMBP report.<br>• Letter of intent to suspend/revoke.<br>• Recommendation to suspend.<br>• Re-instatement with CGD.<br>• 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. Delivery dates for the project milestones will be subject to contract award and start date of the contractor. Should delays occur in the awarding of a contract, project milestone dates will be adjusted accordingly. Adjustment of timelines, if required, will occur upon contract award.

| Key Activities | Completion Date |
|---|---|
| Contract Award | August 2017 |
| Solution 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 Report:
- Assessment of project performance;
- Identification of lessons learned;

- Confirmation that essential contractual and other project closure activities have been completed;
- Outstanding Issues;
- Transfer of assets, deliverables and ongoing administrative functions; and
    - Measurement of post implementation benefits/outcomes (KPI) delivered by the project.

(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 vertical public facing web front-end service.

### 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;<br>2) Update account profile/preferences;<br>3) View guidelines and forms;<br>4) Receive general notification from CSP;<br>5) Send notification to CSP;<br>6) Electronic signature/electronic consent;<br>7) Generate reports;<br>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);<br>2) Submit supporting documentation (as required by CSP);<br>3) Receive case specific notification from CSP;<br>4) Send case specific notification to CSP;<br>5) View case specific documents issued by CSP;<br>6) Track status of Registration/Renewal service requests;<br>7) Search/View past Renewal service requests completed. |
| Personnel Security Screening | 1) Request creation of Applicant accounts;<br>2) Request creation of CSO accounts;<br>3) Submit Requests for Personnel Security Screening services (New, Update, Upgrade, Transfer, Duplication, Re-activation, Termination);<br>4) Complete PSS requests for herself/himself and on behalf of Applicants;<br>5) Track completion status of Personnel Security Screening service requests;<br>6) Send/receive case specific notifications to/from CSP;<br>7) Forward to Applicants case specific notification received from CSP;<br>8) View/Delete/Submit Applicants' supporting documents to CSP;<br>9) View CSP documents (Briefing Certificates, etc.);<br>10) Search past PSS requests completed. |
| Subcontracting | 1) Complete/Update/Submit SRCLs;<br>2) Complete/Update/Submit Private Sector Organization Screening; |

| | |
|---|---|
| | 3) Submit supporting documentation (as required by CSP);<br>4) View case specific documents issued by CSP (e.g., Security Clauses, Subcontractor's organization security clearance and individual clearances, etc.);<br>5) Receive case specific notification from CSP;<br>6) Send case specific notification to CSP;<br>7) Track status of service requests;<br>8) View past service requests (completed). |
| Request for Visit | 1) Submit Request for Visit service requests;<br>2) Submit Amendments (Renewals/Additions/Deletions) to Requests for Visit service requests;<br>3) Submit supporting documentation (as required by CSP);<br>4) View CSP documents (e.g., Authorized Visit request clearance Form, Letter of rejection, etc.);<br>5) Receive case specific notification from CSP;<br>6) Send case specific notification to CSP;<br>7) Track completion status of RFV service requests;<br>8) Search/View past RFV (completed). |
| Documents Transfer | 1) Send notification of documents transfer;<br>2) Submit supporting documentation (as required by CSP);<br>3) Receive case specific notification from CSP;<br>4) View case specific documents issued by CSP;<br>5) Track status of Documents Transfer service request;<br>6) View/Search past Documents Transfer information. |
| Report Security Breaches | 1) Send notification of security breach to CSP;<br>2) Submit supporting documentation (as required by CSP);<br>3) Receive case specific notification from CSP;<br>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;<br>2) Update identification credentials;<br>3) View guidelines and forms;<br>4) Receive general notification from CSP;<br>5) Send notification to CSP;<br>6) Electronic signature/electronic consent;<br>7) Generate reports;<br>8) View/set Calendar events. |
| Sponsor an Organization | 1) Submit Private Sector Organization Screening (PSOS) service requests;<br>2) Submit supporting documentation (as required by CSP);<br>3) Track status of Registration service requests;<br>4) Receive case specific notification from CSP; |

| | |
|---|---|
| | 5) Send case specific notification to CSP;<br>6) View case specific documents issued by CSP;<br>7) Search past Sponsoring service requests (completed). |
| Personnel Security Screening | 1) Request creation/deletion of Applicant accounts;<br>2) Send case specific notification to Applicant;<br>3) Receive case specific notification from Applicant;<br>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;<br>2) Submit Amendments (Renewals/Additions/Deletions) to Requests for Visit service requests;<br>3) Submit supporting documentation (as required by CSP);<br>4) View CSP documents (e.g., Authorized Visit request clearance Form, Letter of rejection, etc.);<br>5) Receive case specific notification from CSP;<br>6) Send case specific notification to CSP;<br>7) Track completion status of RFV service requests;<br>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;<br>2) Update account preferences;<br>3) View guidelines and forms;<br>4) Receive general notification from CSP;<br>5) Electronic signature/electronic consent |
| Personnel Security Screening | 1) Complete Personnel Security Screening Requests online;<br>2) Submit supporting documentation (if required);<br>3) Receive case specific notification from CSO or GC-SO;<br>4) View case specific documents issued by CSO or GC-SO;<br>5) Send case specific notification to CSO or GC-SO;<br>6) Track status of service requests;<br>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;<br>2) Update account profile/preferences;<br>3) Update identification credentials;<br>4) Receive general notification from CSP;<br>5) Send notification to CSP; |

| | |
|---|---|
| | 6) Electronic signature/electronic consent;<br>7) Generate reports<br>8) View/set Calendar events |
| Request for Visit | 1) Submit Request for Visit service requests<br>2) Submit Amendments (Renewals/Additions/Deletions) to Requests for Visit service requests<br>3) Submit supporting documentation (as required by CSP)<br>4) View CSP documents (e.g., Authorized Visit request clearance Form, Letter of rejection, etc.)<br>5) Receive case specific notification from CSP<br>6) Send case specific notification to CSP<br>7) Track completion status of RFV service requests;<br>8) Search/View past RFV (completed) |
| Sponsor an Organization | 1) Submit Private Sector Organization Screening (PSOS) service requests;<br>2) Submit supporting documentation (as required by CSP)<br>3) Track status of Registration service requests<br>4) Receive case specific notification from CSP<br>5) Send case specific notification to CSP<br>6) View case specific documents issued by CSP<br>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<br>2) Update identification credentials<br>3) View guidelines and forms<br>4) Receive general notification from CSP<br>5) Send notification to CSP<br>6) Electronic signature/electronic consent;<br>7) Generate reports<br>8) View/set Calendar events |
| Sponsor an Organization | 1) Submit Private Sector Organization Screening (PSOS) service requests;<br>2) Submit supporting documentation (as required by CSP)<br>3) Track status of Registration service requests<br>4) Receive case specific notification from CSP<br>5) Send case specific notification to CSP<br>6) View case specific documents issued by CSP<br>7) Search past Sponsoring service requests (completed) |
| Contract Security | 1) Complete and submit SRCLs;<br>2) View/Update SRCLs;<br>3) Submit contract information;<br>4) Update contract information (amendments);<br>5) Submit supporting documentation (if required);<br>6) View case specific documents issued by CSP (e.g., Security Clauses);<br>7) Receive case specific notification from CSP; |

| | |
|---|---|
| | 8) Send case specific notification to CSP;<br>9) Track status of service requests;<br>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;<br>2) Update account profile/preferences;<br>3) View guidelines and forms;<br>4) Receive general notification from CGP;<br>5) Send notification to CGP;<br>6) Electronic signature/electronic consent;<br>7) Generate reports;<br>8) View/set Calendar events. |
| Registration | 1) Complete/Maintain Registration in CGP;<br>2) Submit supporting documentation (e.g., Security Assessment Application, etc.);<br>3) Receive case specific notification from CGP;<br>4) Send case specific notification to CGP;<br>5) View case specific documents issued by CGP (e.g., copy of Certificate of Registration, etc.);<br>6) Track status of Registration/Renewal service requests;<br>7) Search/View past Renewal service requests completed; |
| Appointment of DO | 1) Request creation of Designated Official accounts;<br>2) Submit Request for CGP vetting the appointment of a DO;<br>3) Submit supporting documentation (if required);<br>4) Receive case specific notification from CGP;<br>5) Send case specific notification to CGP;<br>6) View case specific documents issued by CGP (e.g., Letter of Acceptance, copy of Designated Official Certification Program certificate, etc.);<br>7) Track status of registration/DO vetting service request;<br>8) Search/View past service requests. |
| Report Security Breaches | 1) Submit Security Breach Report;<br>2) Submit supporting documentation (as required by CGP);<br>3) Receive case specific notification from CGP;<br>4) Send case specific notification to CGP;<br>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;<br>2) Update account profile/preferences;<br>3) View guidelines and forms;<br>4) Receive general notification from CGP;<br>5) Send notification to CGP;<br>6) Electronic signature/electronic consent;<br>7) Generate reports;<br>8) View/set Calendar events. |
| Exemptions from Registration in the CGP | 1) Submit Applications Exemption from Registration (Visitor/Temporary Worker);<br>2) Submit supporting documentation (e.g., Security Assessment Application, etc.)<br>3) Receive case specific notification from CGP;<br>4) Send case specific notification to CGP;<br>5) View case specific documents issued by CGP;<br>6) Track status of Registration/Renewal service requests;<br>7) Search/View past Renewal service requests completed; |
| Referrals to the CGP | 1) Requests CGP assistance in completing employee determination;<br>2) Submit supporting documentation (e.g., Security Assessment Application, proof of citizenship, CRNC, etc.);<br>3) Receive case specific notification from CGP;<br>4) Send case specific notification to CGP;<br>5) View case specific documents issued by CGP;<br>6) Track status of Referral service requests;<br>7) Search/View past Referral service requests completed. |
| Report Security Breaches | 1) Submit Security Breach Report;<br>2) Submit supporting documentation (as required by CGP);<br>3) Receive case specific notification from CGP;<br>4) Send case specific notification to CGP;<br>5) View case specific documents issued by CGP;<br>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 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;<br>2) View case and case information. |
| Processing | 1) Limited service request processing;<br>2) Trigger security partner checks;<br>3) Limited service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request);<br>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);<br>5) Assign case files for further processing;<br>6) Input case notes;<br>7) Attach files of various formats to the case file;<br>8) Close case files. |
| Notifications/<br>Correspondence | 1) Generate and send notifications;<br>2) Generate and send correspondence;<br>3) Attach notifications and correspondence to case file;<br>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;<br>2) View case and case information. |
| Processing | 1) Full service request processing;<br>2) Trigger security partner checks;<br>3) Trigger internal sub processes (e.g. trigger a compliance inspection request);<br>4) Limited service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request);<br>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);<br>6) Open case files that may or may not be linked to existing cases;<br>7) Assign case files for further processing;<br>8) Input case notes;<br>9) Create and manage scheduled activities (e.g. inspectors create blocks of inspections within geographical areas to maximize travel costs);<br>10) Attach files of various formats to the case file;<br>11) Close case files. |
| Notifications/<br>Correspondence | 1) Generate, edit and send notifications;<br>2) Generate, edit and send correspondence;<br>3) Attach notifications and correspondence to case file;<br>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;<br>2) View case and case information. |
| Processing | 1) Full service request processing;<br>2) Trigger security partner checks;<br>3) Trigger internal sub processes (e.g. trigger a compliance inspection request);<br>4) Service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request);<br>5) Edit service request processing information, no modification to data submitted with the service request;<br>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);<br>7) Open case files that may or may not be linked to existing cases.<br>8) Assign case files for further processing;<br>9) Input case notes;<br>10) Edit existing case notes;<br>11) Create and manage scheduled activities (e.g. inspectors create blocks of inspections within geographical areas to maximize travel costs);<br>12) Attach files of various formats to the case file;<br>13) Manage supporting documents and files attached to case files;<br>14) Close case files. |
| Notifications/<br>Correspondence | 1) Generate, edit and send notifications;<br>2) Modify notification templates;<br>3) Generate, edit and send correspondence;<br>4) Modify correspondence templates;<br>5) Attach notifications and correspondence to case file;<br>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);<br>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;<br>2) View case and case information. |
| Processing | 1) Assign case files for further processing;<br>2) Input case notes;<br>3) Edit existing case notes;<br>4) Attach files of various formats to the case file;<br>5) Manage supporting documents and files attached to case files;<br>6) Service request modification (e.g. modification to service request prioritization level, no modification to data submitted with the service request);<br>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/<br>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 );<br>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;<br>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;<br>2) View case and case information. |
| Maintenance | 1) Create and edit notification templates;<br>2) Create and edit correspondence templates;<br>3) Create, disable, delete and modify user accounts (e.g. user account tombstone information);<br>4) Add or remove available capabilities or roles to user accounts;<br>5) Add, modify, delete or disable capabilities that are available to be assigned to a user role;<br>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;<br>7) Add, modify, delete or disable, workflows within the solution;<br>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);<br>9) Modify externally facing forms and publish them to the solutions web portal;<br>10) Add, modify, delete or disable whole or parts of the solution;<br>11) Maintain access control and permissions at the field level at the user role level;<br>12) Update a sandbox environment with a copy of the solution from production (application only, no data);<br>13) Ability to enable/disable a link displayed on the solutions web portal (Business Requirement APP-OPS.22);<br>14) Maintain access to the various environments used to support the solution. |
| Reporting<br>Maintenance | 1) Generate available predetermined reports.<br>2) Add, modify, delete or disable reports available within the solution;<br>3) Add, modify, delete or disable selection criteria associated to a report;<br>4) Add, modify, delete or disable reports that can be accessed by user roles and/or user accounts;<br>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. |

# 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).

# 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 vertical public facing web front-end service 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 vertical public facing web front-end service
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.

**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

**SABA:** A talent Management Software Solution that offers Learning Management (LMS), Performance Management and Cloud Collaboration.

**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.<br>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

**Vertical Public Facing Web Front-End Service:** 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 vertical public facing web front-end service include intranet "dashboards" for executives and managers.

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**<br>*(start/end dates to be inserted at award)*<br>**Firm All-Inclusive Per Diem Rate (CDN $)** | **Option Periods 1, 2, 3, and 4**<br>*(start/end dates to be inserted at award)*<br>**Firm All-Inclusive Per Diem Rate (CDN $)** |
| 1. Communications Consultant (Level 3) | | |
| 2. Courseware Developer (Level 3) | | |
| 3. Data Conversion Specialist (Level 3) | | |
| 4. Database Administrator (Level 3) | | |
| 5. Database Modeller / IM Modeler (Level 3) | | |
| 6. Information Management Architect (Level 3) | | |
| 7. Programmer / Analyst – Business Objects (Level 3) | | |
| 8. Programmer / Analyst – MS Dynamcis CRM (Level 3) | | |
| 9. Web Developer (Level 3) | | |
| 10. Business Process Re-engineering (BPR) Consultant (Level 3) | | |
| 11. Change Management Consultant (Level 3) | | |
| 12. Cybersecurity Specialist (Level 3) | | |
| 13. Incident Management Specialist (Level 3) | | |
| 14. IT Security Design Specialist (Level 3) | | |
| 15. IT Security Engineer (Level 3) | | |
| 16. IT Security VA Specialist (Level 3) | | |
| 17. Network Analyst (Level 3) | | |
| 18. Operations Support Specialist (Level 3) | | |
| 19. System Auditor (Level 3) | | |
| 20. Testing Coordinator (Level 3) | | |
| 21. Web Designer (Level 3) | | |
| 22. Programmer / Software Developer (Level 3) | | |

| **Table 2 - As-and-When-Requested Work (Section 9 of ANNEX A - SOW) – Task Authorizations – Resource Categories (Continued)** | | |
|---|---|---|
| **Resource Categories** | **Initial Contract Period**<br>*(start/end dates to be inserted at award)*<br>**Firm All-Inclusive Per Diem Rate (CDN $)** | **Option Periods 1, 2, 3, and 4**<br>*(start/end dates to be inserted at award)*<br>**Firm All-Inclusive Per Diem Rate (CDN $)** |
| 23. Application/Software Architect (Level 3) | | |
| 24. Database Analyst (Level 3) | | |

# 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:

1. Communications Consultant (Level 3);
2. Courseware Developer (Level 3);
3. Data Conversion Specialist (Level 3);
4. Database Administrator (Level 3);
5. Database Modeller (Level 3);
6. Information Management (IM) Architect (Level 3);
7. Programmer / Analyst – Business Objects (Level 3);
8. Programmer / Analyst - MS Dynamics CRM (Level 3);
9. Web Developer (Level 3);
10. Business Process Re-engineering (BPR) Consultant (Level 3);
11. Change Management Consultant (Level 3);
12. Cybersecurity Specialist (Level 3);
13. Incident Management Specialist (Level 3);
14. IT Security Design Specialist (Level 3);
15. IT Security Engineer (Level 3);
16. IT Security VA Specialist (Level 3);
17. Network Analyst (Level 3);
18. Operations Support Specialist (Level 3);
19. System Auditor (Level 3);
20. Testing Coordinator (Level 3);
21. Web Designer (Level 3);
22. Programmer / Software Developer (Level 3);
23. Application / Software Architect (Level 3); and
24. Database Analyst (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 web technologies. |

## 3.10 Business Process Re-engineering (BPR) Consultant (Level 3)

### 3.10.1 Required Services

The required services may include, but are not limited to the following:

a) Review existing work processes and organizational structure.
b) Analyze business functional requirements to identify information, procedures and decision flows.
c) Identify candidate processes for re-design; prototype potential solutions, provide trade-off information and suggest a recommended course of action. Identify the modifications to the automated processes.

d) Provide expert advice in defining new requirements and opportunities for applying efficient and effective solutions; identify and provide preliminary costs of potential options.
e) Provide expert advice in developing and integrating process and information models between processes to eliminate information and process redundancies.
f) Identify and recommend new processes and organizational structures.
g) Provide expert advice on and assist in implementing new processes and organizational changes.
h) Document workflows.
i) Use business, workflow and organizational modeling software tools.

### 3.10.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Business Process Re-engineering Consultant. |
| M2 | 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) and (g) of 3.10.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.11 Change Management Consultant (Level 3)

### 3.11.1 Required Services

The required services may include, but are not limited to the following:

a) Designing interventions aimed at improving organizational effectiveness through system-centered change;
b) Designing interventions that improve organizational effectiveness through people-centered change and result in: bringing about change, an improved environment, greater involvement and a more responsive workforce;
c) Developing and implementing change management strategies, plans, framework;
d) Identifying change management tools and risks;
e) Providing expertise, consultative advice, guidance and coaching to build project capacity to make effective use of change management strategies and related tools;
f) Articulating the purpose of change in a manner that makes sense to staff and provides a compelling picture of the new organization;
g) Designing and conducting a change readiness assessment in order to plan and carry out a change management strategy;
h) Coaching staff on the value of their contribution within the new organization;
i) Evaluating the effectiveness of the change management initiative.
j) Developing performance measurement/evaluation frameworks;
k) Integrating performance monitoring disciplines in an organization's development or change management plan; and
l) Carrying out performance monitoring and reporting activities on change management.

### 3.11.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Change Management Consultant. |
| M2 | 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), (g), (i), (j) and (k) of 3.11.1. |

## 3.12 Cybersecurity Specialist (Level 3)

### 3.12.1 Required Services

The required services may include, but are not limited to the following:

a) Develop Security Solution Design (High-Level and Detail-level);
b) Develop Security Plans such as: Security Installation Plan; Security Testing Plan; Security Installation Verification Plan; Vulnerability Assessment Plan;
c) Conduct TRA activities throughout the Solution Development Life Cycle;
d) Develop Procedures such as: Operational Security Procedures; Security Installation Procedures;
e) Develop and maintain the Security Requirements Traceability Matrix;
f) Prepare security reports such as TRA report(s), Security Installation Verification Reports, Security Integration Test Report
g) Prepare IT Security packages for SA&A gating
h) Train developers on secure coding practices to embed knowledge of security into the development process

### 3.12.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as an IT Security Specialist. |
| M2 | Must have a minimum of five (5) years of experience, within the last 10 (ten) years performing the responsibilities described at (a), (b), (c) and (d) of 3.12.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.13 Incident Management Specialist (Level 3)

### 3.13.1 Required Services

The required services may include, but are not limited to the following:

(a) Review, analyze, and apply:
  - Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap
  - Reporting and resolution procedures for IT Security incidents (for example DOS attacks) and International IT Security incident advisory services
  - Networking Protocols such as HTTP, FTP, Telnet
  - Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH

- TCP/IP, UDP, DNS, SMTP, SNMP
- Intrusion detection systems, firewalls, content checkers and antivirus software
- Network infrastructure components, such as multiplexers, routers/hubs, switches

(b) Provide incident analysis support, including:

- Response mechanisms
- Co-ordination of all prevention and response plans
- Emergency Operations Centre (EOC) activities
- Co-ordination with the national Integrated Threat Assessment Centre and Government Operations Centre
- Participation in the Integrated National Security Framework and National Cyber Security Strategy

(c) Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses
(d) Conduct on-site reviews and analysis of system security logs
(e) Produce system activity reports, logs and incident analysis
(f) Assist in managing and running an incident response centre
(g) Complete tasks directly supporting the departmental IT Security and Cyber Protection Program
(h) Develop and deliver training material relevant to the resource category

### 3.13.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience in Incident Management. |
| M2 | 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 (e) of 3.13.1 |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.14 IT Security Design Specialist (Level 3)

### 3.14.1 Required Services

The required services may include, but are not limited to the following:

a) Review, analyze, and apply: Architectural methods, frameworks, and models such as TOGAF, US government FEAP, Canadian government BTEP and GSRM, Zachman, UMM
b) Review, analyze, and apply a broad range of security technologies including multiple types of systems and applications architectures, and multiple hardware and software platforms, including:

- Directory Standards such as X.400, X.500, and SMTP
- Operating Systems such as MS, Unix, Linux, and Novell
- Networking Protocols (e.g., HTTP, FTP, Telnet)
- Network routers, multiplexers and switches
- Domain Name Services (DNS) and Network Time Protocols (NTP)

c) Review, analyze, and apply Secure IT architectures, standards, communications, and security protocols such as IPSec, SSL, SSH, S-MIME, HTTPS
d) Review, analyze, and apply IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) stacks
e) Review, analyze, and apply the significance and implications of market and technology trends in order to apply them within architecture roadmaps and solution designs. (examples: web services security, incident management, identity management)
f) Review, analyze, and apply Best practices and standards related to the concept of network zoning and defence in-depth principles
g) Review, analyze, and apply IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) stacks
h) Analyze IT Security statistics, tools and techniques
i) Analyze security data and provide advisories and reports
j) Prepare technical reports such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling
k) Brief senior managers
l) Security architecture design and engineering support
m) Conduct data security designation/classification studies
n) Prepare tailored IT Security alerts and advisories from open and closed sources Complete tasks directly supporting the departmental IT Security and Cyber Protection Program
o) Develop and deliver training material relevant to the resource category

### 3.14.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as an IT Security Specialist. |
| M2 | 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), (g), (l), (m) and (n) of 3.14.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.15 IT Security Engineer (Level 3)

### 3.15.1 Required Services

The required services may include, but are not limited to the following:

(a) Review, analyze and apply:
- Directory Standards such as X.400, X.500, and SMTP
- Operating Systems such as MS, Unix, Linux, and Novell
- Networking Protocols such as HTTP, FTP, and Telnet
- Secure IT architectures fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, and SSH
- IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control
- Protocol/Internet Protocol (TCP/IP) stacks
- Domain Name Services (DNS) and Network Time Protocols (NTP)

- Network routers, multiplexers and switches
- Application, host and Network hardening and security best practices such as shell scripting, service identification, and access control
- Intrusion detection/prevention systems, malicious code defence, file integrity, Enterprise Security Management and firewalls
- Wireless technology
- Cryptographic Algorithms

(b) Identify the technical threats to, and vulnerabilities of, networks
(c) Manage the IT Security configuration
(d) Analyze IT Security tools and techniques
(e) Analyze the security data and provide advisories and reports
(f) Analyze IT Security statistics
(g) Prepare technical reports such as IT Security Solutions option analysis and implementation plans
(h) Provide Independent Verification and Validation (IV&V) support to IT Security related projects including:

- IT Security audits, including applicable reports, presentations and other documentation,
- Review of contingency plans, Business Continuity Plans and Disaster Response Plans
- Design/development and conduct IT Security protocols tests and exercises
- Project oversight

(i) Develop and deliver training material relevant to the resource category

### 3.15.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as an IT Security Specialist. |
| M2 | 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), (f) and (h) of 3.15.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.16 IT Security VA Specialist (Level 3)

### 3.16.1 Required Services

The required services may include, but are not limited to the following:

(a) Review, analyze, and apply:

- Threat agents analysis tools and other emerging technologies including privacy enhancement, predictive analysis, VoIP, data visualization and fusion, wireless security devices, PBX and telephony firewall
- War dialers, password crackers
- Public Domain IT vulnerability advisory services
- Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap
- Networking Protocols (HTTP, FTP, Telnet)
- Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP

- Wireless Security
- Intrusion detection systems, firewalls and content checkers
- Host and network intrusion detection and prevention systems - Anti-virus management

(b) Identify threats to, and technical vulnerabilities of, networks
(c) Conduct on-site reviews and analysis of system security logs
(d) Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses
(e) Prepare and deliver IT Security threat, vulnerability and risk briefings
(f) Completed tasks directly supporting the departmental IT Security and Cyber Protection Program
(g) Develop and deliver training material relevant to the resource category

### 3.16.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as an IT Security Specialist. |
| M2 | 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 3.16.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.17 Network Analyst (Level 3)

### 3.17.1 Required Services

The required services may include, but are not limited to the following:

(a) Prepare implementation plans for particular technologies.
(b) Installs and monitors particular facets of technology.
(c) Configures and optimizes technical installations.
(d) Troubleshoots, and responds to user problems.
(e) Maintain up to date knowledge of particular technologies and products supporting that technology.

### 3.17.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Network Analyst. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a) to (e) of 3.17.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.18 Operations Support Specialist (Level 3)

### 3.18.1 Required Services

The required services may include, but are not limited to the following:

(a) Provide systems administration and systems operations support, including setting up user access, user profiles, back up and recovery, day-to-day computer systems operations.
(b) Perform software upgrades, and apply patches.
(c) Provide customer interface to ensure requested changes are implemented.
(d) Monitor computer workload trends and make adjustments to ensure optimum utilization of computer resources.

### 3.18.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience in Operations Support. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a) to (d) of 3.18.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.19 System Auditor (Level 3)

### 3.19.1 Required Services

The required services may include, but are not limited to the following:

(a) Review organizational IT policy, standards and procedures and provide advice on their adequacy.
(b) Conduct systems under development reviews by reviewing project documentation, conducting interviews, assessing work completed, and, based on findings, reporting on compliance with policy, standards and procedures, and progress against plan.
(c) Conduct reviews of systems recently implemented and reporting on:
  - benefits actually achieved versus projected benefits,
  - features actually delivered versus stated requirements,
  - the adequacy of controls and system security features,
  - user satisfaction based on surveys or interviews,
  - system performance and reliability.
(d) Review systems that have been in production status for some time and report on issues, deficiencies, and shortcomings.

### 3.19.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a System Auditor. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a) to (d) of 3.19.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.20 Testing Coordinator (Level 3)

### 3.20.1 Required Services

The required services may include, but are not limited to the following:

a) Provide advice, guidance and coordination efforts for test strategies and plans, selection of automated testing tools, and identification of resources required for testing.
b) Plan, organize, and schedule testing efforts for large systems, including the execution of systems integration tests, specialized tests, and user acceptance testing (e.g., stress tests).

### 3.20.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Testing Coordinator. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a) and (b) of 3.20.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.21 WEB Designer (Level 3)

### 3.21.1 Required Services

The required services may include, but are not limited to the following:

a) Define architecture to be used in the web-based projects.
b) Create and apply designs that maximize usability of existing objects.
c) Perform architectural modeling to ensure consistency of the design with existing work.
d) Select the development language to be used for the project.
e) Assess the impact of the new requirements on existing web applications.
f) Develop code based upon design and requirements documents.
g) Write code to write to and read from the database.
h) Unit test the code prior to releasing it for integration testing.
i) Monitor the need for design changes as the project progresses.
j) Develop test plans for testing the system.
k) Ensure functionalities have been implemented according to specifications.
l) Define assumptions and constraints of architecture with regard to physical structure and data collection.
m) Develop post-implementation plan for monitoring/tracking design stability.

### 3.21.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Web Designer. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (c), (e), (f), (g), (k), (l) and (m) of 3.21.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

## 3.22 Programmer / Software Developer (Level 3)

### 3.22.1 Required Services

The required services may include, but are not limited to the following:

a) Develop and prepare diagrammatic plans for solution of business, scientific and technical problems by means of computer systems of significant size and complexity.
b) Analyze the problems outlined by the systems analysts/designers in terms of such factors as style and extent of information to be transferred to and from storage units, variety of items to be processed, extent of sorting, and format of final printed results.
c) Select and incorporate available software programs.
d) Design detailed programs, flow charts, and diagrams indicating mathematical computation and sequence of machine operations necessary to copy and process data and print the results.
e) Translate detailed flow charts into coded machine instructions and confer with technical personnel in planning programs.
f) Verify accuracy and completeness of programs by preparing sample data, and testing them by means of system acceptance test runs made by operating personnel.
g) Correct program errors by revising instructions or altering the sequence of operations.
h) Test instructions, and assemble specifications, flow charts, diagrams, layouts, programming and operating instructions to document applications for later modification or reference.

### 3.22.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Programmer / Software Developer. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (b) and (d) of 3.22.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

### 3.23 Application / Software Architect (Level 3)

#### 3.23.1 Required Services

The required services may include, but are not limited to the following:

a) Develop technical architectures, frameworks and strategies, either for an organization or for a major application area, to meet the business and application requirements.
b) Identify the policies and requirements that drive out a particular solution.
c) Analyze and evaluate alternative technology solutions to meet business problems.
d) Ensures the integration of all aspects of technology solutions.
e) Monitor industry trends to ensure that solutions fit with government and industry directions for technology.
f) Analyze functional requirements to identify information, procedures and decision flows.
g) Evaluate existing procedures and methods, identify and document database content, structure, and application sub-systems, and develop data dictionary.
h) Define and document interfaces of manual to automated operations within application sub-systems, to external systems and between new and existing systems.
i) Define input/output sources, including detailed plan for technical design phase, and obtain approval of the system proposal.
j) Identify and document system specific standards relating to programming, documentation and testing, covering program libraries, data dictionaries, naming conventions, etc.

#### 3.23.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as an Application / Software Architect. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a), (c), (d), (g) and (i) of 3.23.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

### 3.24 Database Analyst (Level 3)

#### 3.24.1 Required Services

The required services may include, but are not limited to the following:

a) Define new database structures.
b) Define data conversion strategy.
c) Define database conversion specifications.
d) Finalize Conversion Strategy.
e) Work very closely with the users in order to maintain and safeguard the database.

f) Identify requirements for improvements to existing databases by determining users' information requirements and system performance and functional requirements.
g) Develop and implement procedures that will ensure the accuracy, completeness, and timeliness of data stored in the database.
h) Mediates and resolves conflicts among users' needs for data.
i) Advise programmers, analysts, and users about the efficient use of data.

### 3.24.2 Minimum Mandatory Qualifications

| No. | Description of Criteria |
|---|---|
| M1 | Must have a minimum of ten (10) years of experience as a Database Analyst. |
| M2 | Must have a minimum of five (5) years of experience, within the last ten (10) years, performing the responsibilities described at (a) to (i) of 3.24.1. |
| M3 | Must have a minimum of three (3) years of experience, within the last ten (10) years, developing web based service delivery. |

# 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. For the purposes of this evaluation, the Bidder should assume the timelines that are currently provided within Appendix 2 of Annex A.

| 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 | 160 | |
| R4 | Security Management | 360 | |
| R5 | Sensitive Data Migration | 200 | |
| R6 | Change Management Plan | 380 | |
| R7 | Testing Plan | 160 | |
| R8 | Corporate Reference Projects: Government of Canada Client | 80 | |
| R9 | Corporate Reference Projects: Case Management, Microsoft Dynamics CRM and Vertical Public Facing Web Front-End Services | 180 | |
| **Maximum Total Points for Point Rated Criteria** | | **2500** | |
| **Minimum Pass Mark for Point Rated Criteria (70%)** | | **1750** | |

Note: *Refer to the Generic Technical Evaluation Scale included at section 4 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 purposes 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.

<table>
<tr><th>ID</th><th>Mandatory Requirement</th><th>Cross Reference to Bidder's Proposal</th></tr>
<tr><td>M1</td><td>

**Corporate Reference Projects: Business Process Re-Engineering and Change Management**

The Bidder must provide **three (3)** Reference Projects in total. **Two (2) of the three (3)** Reference Projects must be similar to that of ANNEX A, Sections 2 through 7. All Reference Projects must have been completed within **fifteen (15)** years of the date of Bid Closing and must have had a public-facing internet-based information exchange component. For all 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 having at least 65% of the number of user accounts and at least 65% of the number of and diversity of transactions as indicated in ANNEX A, Section 1, 3.1, Volumetric Data. If a project's solution was designed and developed to service an intended volume of user accounts, number of transactions and diversity of transactions that meet the minimums, identified in the table below, then this project can be used as a Reference Project. Note that the anticipated volumes must have remained greater than the identified minimums throughout the duration of the project.

<table>
<tr><th>Metric</th><th>RFP</th><th>Minimum for Project Reference</th></tr>
<tr><td>User Accounts – Internal & External</td><td>184,392</td><td>119,854</td></tr>
<tr><td>Number of transactions for Registration, Screening and Clearances</td><td>209,469</td><td>136,154</td></tr>
<tr><td>Diversity of Transactions</td><td>12</td><td>7</td></tr>
</table>

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<br>
ii. Developing a communication plan<br>
iii. Delivering communication plan

</td><td></td></tr>
</table>

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 and must be similar to that of ANNEX A, Sections 2 through 7 as defined above.

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 contract closeout);
v. Description of users;
vi. Volumetrics, including number of user accounts, number of 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 in total. **Two (2) of the three (3)** Reference Projects must be similar to that of ANNEX A, Sections 2 through 7. All Reference Projects must have been completed within **fifteen (15)** years of the date of Bid Closing and must have had a public-facing internet-based information exchange component. For all 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 for at least one Reference Project.

For the purpose of this evaluation, a similar project would be defined as having at least 65% of the number of user accounts and at least 65% of the number of and diversity of transactions as indicated in ANNEX A, Section 1, 3.1, Volumetric Data. If a project's solution was designed and developed to service an intended volume of user accounts, number of transactions and diversity of transactions that meet the minimums, identified in the table below, then this project can be used as a Reference Project. Note that the anticipated volumes must have remained greater than the identified minimums throughout the duration of the project.

| **Metric** | **RFP** | **Minimum for Project Reference** |
|---|---|---|
| User Accounts – Internal & External | 184,392 | 119,854 |

| | | |
|---|---|---|
| Number of transactions for Registration, Screening and Clearances | 209,469 | 136,154 |
| Diversity of Transactions | 12 | 7 |

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 user accounts, number of and diversity of transactions; and
   vii. 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 and the Reference Project must be similar to that of ANNEX A, Sections 2 through 7 as defined above.

D. 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.

E. For at least one (1) Reference Project, the Bidder completed a vertical public facing web front-end service solution that was implemented and integrated with a back end processing solution for information exchange. The solution must have had security requirements similar to those identified in ANNEX A, Section 5, 1.2. IT Security Requirements. For the purpose of this evaluation, similar IT security requirements would be defined as having implemented a solution that uses sensitive data (Protected B) and requires the protection of data integrity. The Referenced Project must also be similar to that of ANNEX A, Sections 2 through 7 as defined above.

| | | |
|---|---|---|
| **M3** | **Customer References**<br>For each Reference Project provided in response to M1 and M2, the Bidder must complete Form 2 to Part 4. The client contact may be contacted to validate the information provided in the Bidder's response, in accordance with Part 4.2.4, Reference Checks. | |

## 4. 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**<br><br>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 should align to the National Project Management System (NPMS) framework.<br><br>Canada will evaluate the Bidder's Preliminary 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: | **Maximum Points: 620** | |
| | A. **Project Governance and Team Structure**, including the following: | Part A : Maximum Points : 60 | |
| | i. Roles and responsibilities matrix including the Contractor and GC; | i. Maximum Points: 20 | |
| | ii. Description of the high-level project team structure and relationships (highlighting groups and entities that form the project team); and | ii. Maximum Points: 20 | |
| | iii. Diagram of the governance model that will be employed by the Bidder for this project. | iii. Maximum Points: 20 | |
| | B. **Scope Management** describing how scope will be managed throughout the Project Delivery Stage. This narrative should address the following: | Part B Maximum Points: 140 | |
| | 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 | i. Maximum Points: 70 | |
| | ii. A description of how scope will be managed throughout the Project Delivery Stage. This should 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. | ii. Maximum Points: 70 | |
| | C. **Schedule Management** that outlines the Bidder's strategy for managing ISST project activities. The response should contain the following: | Part C Maximum Points: 80 | |
| | i. For each project activity and milestone, the associated deliverables including the critical path used to achieve said deliverables; | i. Maximum Points: 45 | |
| | ii. Mitigation measures and strategies to handle schedule deviations. | ii. Maximum Points: 35 | |
| | D. **Project Schedule** that outlines the activities and timelines for the project. The response should contain the following: | Part D Maximum Points: 70 | |
| | i. WBS denomination at [minimum] 2 levels (in addition to the project context): The WBS should identify all major work packages required to deliver the project; | i. Maximum Points: 35 | |
| | ii. Estimated duration for each activity, and dependencies (predecessors); | ii. Maximum Points: 35 | |
| | The Project Schedule is requested to be delivered in MS Project 2013 or higher and should address the constraints identified throughout ANNEX A. The schedule should assume a start date of September 1, 2017 and respect a production launch date of March 31, 2019. | | |
| | E. **Risk Management**, in alignment with NPMS that includes the following: | Part E Maximum Points: 150 | |

| | | | |
|---|---|---|---|
| | i. A description of the process for identifying, analyzing, and prioritizing project risks;<br>ii. The methods that will be used to track risks, evaluate changes in individual risk exposures, and respond to those changes;<br>iii. Risk management roles and responsibilities; and<br>iv. A list of five (5) project risks and proposed mitigation strategies.<br><br>F. **Quality Management** 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:<br>i. A description of the processes for Quality Planning, Quality Assurance and Quality Control;<br>ii. Methods, tools and techniques that will be used for Quality Management;<br>iii. Quality Management roles and responsibilities;<br>iv. Outline an approach to address quality non-compliance. | i. Maximum Points: 30<br>ii. Maximum Points: 40<br>iii. Maximum Points: 30<br>iv. Maximum Points: 50<br><br>Part F Maximum Points : 120<br><br>i. Maximum Points : 40<br>ii. Maximum Points : 30<br>iii. Maximum Points: 30<br>iv. Maximum Points: 20 | |
| **R2** | **Business Process Re-engineering**<br><br>The Bidder should provide a preliminary Business Process Re-engineering strategy.<br><br>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:<br><br>A. An understanding of the current ISS business processes and the need for security practices within the various business operations;<br><br>B. A plan to conduct a business process gap analysis;<br><br>C. An understanding of constraints and impacts;<br><br>D. Four examples of opportunities to improve process efficiency and effectiveness and proposed implementation approaches;<br><br>E. An understanding of risks and options for risk resolution or mitigation; and<br><br>F. Scheduling of business process re-engineering activities. | **Maximum Points: 360**<br><br>Part A Maximum Points: 60<br>Part B Maximum Points: 50<br>Part C Maximum Points: 40<br>Part D Maximum Points: 60 (Maximum 15 points for each element)<br>Part E Maximum Points: 50<br>Part F Maximum Points: 100 | |
| **R3** | **Relationship Management**<br><br>The Bidder should describe their approach to Relationship Management.<br><br>Canada will evaluate the degree to which the Bidder's response considers the following elements:<br><br>A. Overall approach to Government of Canada and Contractor relationship management;<br><br>B. Communications between the Government of Canada and the Contractor in respect to a proposed governance model and team structure as detailed in R1. A.;<br><br>C. Issue management and resolution;<br><br>D. Joint planning and managing of changes to project scope and schedule. | **Maximum Points : 160**<br><br>Part A Maximum Points : 50<br><br>Part B Maximum Points : 25<br><br>Part C Maximum Points: 35<br><br>Part D Maximum Points : 50 | |

| | | | |
|---|---|---|---|
| R4 | **Security Management**<br>The Bidder should provide, for two (2) operational scenarios, a description of the necessary security considerations for steady-state operations as required for the ISST solution. The response should contain sufficient information to be considered an end to end description for that particular scenario. The document should highlight the requirements for security as indicated in the Security Requirements section of ANNEX A, Section 4.<br>The Bidder should respond in a format for a Concept of Security Operations (SecConOps) document typical for industry usage. A Table of Contents will not be provided.<br>For the purposes of this evaluation, Operational Scenario is defined as a single activity or group of activities that are related and are required to complete a process within the potential solution. Each scenario used in this response, requires consideration of all of the Security Controls referenced in A, B, C, D, below.<br>Examples of "Operational Scenarios" include, but are not limited to:<br>a. describe, the end to end movement of a single message from within Dynamics CRM to a third party recipient;<br>b. describe the scenario of an ISS Field Inspector completing an on-site inspection and submitting the final document to the Dynamics CRM based solution;<br>c. describe the ETL extraction of data for the purposes of Business Intelligence Reporting;<br>d. describe the provision of a single users credentials;<br>e. describe the submission of a user completed service request (excluding ISS processing); and<br>f. describe the process to move a recently completed case to the "solution" archive.<br>Despite the fact that actual implementation of some of the activities described may fall under other Government of Canada group's responsibilities, the Bidder should assume for the purposes of this response and this response only, that they will be responsible for all aspects for the implementation of the operational scenarios of their choice. It is important that all points be addressed even if deemed not applicable. Non-applicable items should contain Bidder reasoning for their non-applicability.<br>Canada will evaluate the degree to which the Bidder's approach to security management reflects the required security controls. In particular, the approach should :<br>A. Reference and address all parts of SC.47 General;<br>B. Reference and address all parts of SC.16 Information Security Architecture; and<br>C. Reference and address all parts of SC.09(a) Information Systems Connections; and<br>D. Reference and Address all parts of SC.42 Security Test Plan. | **Maximum Points : 360**<br>Part A Maximum Points : 90<br>SC.47 a) Three sub parts, 10 pts each<br>SC.47 b) Fifteen sub parts, 4 pts each<br>Part B Maximum Points : 120<br>SC.16 Three sub parts, 40 pts each<br>Part C Maximum Points: 75<br>SC.9 a) One part, 75 pts<br>Part D Maximum Points : 75<br>SC.42 a) One part, 26 pts<br>SC.42 b) One part, 25 pts<br>SC.42 c) Four sub parts, 6 pts each | |
| R5 | **Sensitive Data Migration**<br>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).<br>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:<br>A. An approach to data migration listing key activities to be undertaken; | **Maximum Points: 200**<br>Part A Maximum Points: 70 | |

| | | | |
|---|---|---|---|
| | B. The defined roles, responsibilities, and expectations of the Bidder and Canada;<br>C. The risks and mitigation strategies specifically related to migration activities;<br>D. Activities during data migration which will help satisfy the ITSG-33 based security requirements located within the Security Requirements table, specifically:<br>i. SC-21 Protection of Information;<br>ii. SC-23 Information System Monitoring;<br>iii. SC-28 Information System Recovery and Reconstitution; and<br>iv. SC-31 Information Input Validation.<br>v. SC-44 Security - General | Part B Maximum Points: 40<br>Part C Maximum Points: 40<br>Part D Maximum Points: 50 (Maximum 10 points for each element) | |
| **R6** | **Change Management Plan**<br>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.<br>Canada will evaluate the degree to which the Bidder's Preliminary Change Management Plan supports the successful transition from "as-is" to "to be" states and demonstrates:<br>A. A comprehensive understanding of the Change Management requirements;<br>B. Consideration of the following:<br>i. Avoidance of disruption of service to Canadians;<br>ii. Facilitation of the adoption of process and terminology transitions for all end users, including external users and internal staff;<br>iii. Appropriate, accurate and timely use and input to the new system; and<br>iv. The quality and integrity of the services rendered.<br>C. A comprehensive evaluation method for assessing effectiveness of change management activities. | **Maximum Points: 380**<br>Part A Maximum Points: 100<br>Part B Maximum Points: 200<br>i. Maximum Points: 50<br>ii. Maximum Points: 50<br>iii. Maximum Points: 50<br>iv. Maximum Points: 50<br>Part C Maximum Points: 80 | |
| **R7** | **Testing Plan**<br>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.<br>Canada will evaluate the degree to which the Bidder's test plan demonstrates:<br>A. Due consideration of related Security requirements from SC-42 Security Integration Test Plan as well as Section 6 of ANNEX A;<br>B. Adequate test coverage to ensure Solution go-live readiness. Due consideration of and reference to :<br>i. Integration testing;<br>ii. Functional and non-functional Testing, including Security Testing;<br>iii. Data Validation Testing;<br>iv. Client acceptance testing.<br>C. The identification of risk and its management. | **Maximum Points: 160**<br>Part A Maximum Points: 40<br>Part B Maximum Points: 100 (Maximum 25 points for each element)<br>Part C Maximum Points: 20 | |
| **R8** | **Corporate Reference Projects: Government of Canada Client**<br>The Bidder should provide up to three (3) Reference Projects where it has successfully delivered an IT solution for a Government of Canada client. Reference Projects can include projects provided in response to the Mandatory Criteria where appropriate. Bidders are requested to complete Form 2 to Part 4 for all Reference Projects provided in response to R8. The client contact may be contacted to validate the information provided in the Bidder's response, in accordance with Part 4.2.4, Reference Checks. | **Maximum Points: 80**<br>One (1) Reference Project: 30<br>Two (2) Reference Projects: 50 | |

| | | | |
|---|---|---|---|
| | | Three (3) Reference Projects: 80 | |
| **R9** | **Corporate Reference Projects: Case Management, Microsoft Dynamics Client Relationship Management and Vertical Public Facing Web Front-End Services**<br>The Bidder should provide up to three (3) Reference Projects which will be evaluated in relation to items A, B and C, below.<br>A. Reference Projects that have successfully delivered a solution, requiring both IT design and configuration, using a Case Management solution.<br>B. Reference Projects that have successfully delivered a solution requiring both IT design and configuration, using Microsoft Dynamics CRM 2015 (or higher) for the solution.<br>C. Reference Projects that have successfully delivered a solution requiring IT design, configuration, and integration of vertical public facing web front-end services for information exchange with a Microsoft Dynamics 2015 or higher solution.<br>For the purposes of the 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.<br>Bidders are encouraged to provide Reference Projects that are able to meet the criteria for the evaluation points in order to maximize their score. Reference Projects can include projects that were used as reference for the Mandatory Criteria where appropriate. Bidders are requested to complete Form 2 to Part 4 for all Reference Projects provided in response to R9. The client contact may be contacted to validate the information provided in the Bidder's response, in accordance with Part 4.2.4, Reference Checks.<br>For Example, if a Bidder provides three Reference Projects where Criteria A is satisfied by all three references, Criteria B is satisfied by two of the three references and Criteria C is satisfied by only one of the three references, the Bidder would receive a total of 150 of the maximum 180 points for Evaluation Criteria R9. | **Maximum Points: 180**<br>Maximum Points for A: 60<br>One (1) Reference Project: 40<br>Two (2) Reference Projects: 50<br>Three (3) Reference Projects: 60<br>Maximum Points for B: 60<br>One (1) Reference Project: 40<br>Two (2) Reference Projects: 50<br>Three (3) Reference Projects: 60<br>Maximum Points for C: 60<br>One (1) Reference Project: 40<br>Two (2) Reference Projects: 50<br>Three (3) Reference Projects: 60 | |

| **Reference** | **Criteria A** | **Criteria B** | **Criteria C** | **Total R9 Score** |
|---|---|---|---|---|
| 1 | X | -- | -- | |
| 2 | X | X | -- | |
| 3 | X | X | X | |
| Criteria Total | 60 | 50 | 40 | 150 |

# FORM 3 TO PART 4 – BID SOLICITATION FORM - FINANCIAL BID FORM

## 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 $8,000,000.00 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. <u>As-and-when-requested work:</u>**

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)**<br>Initial Contract Period Firm All-Inclusive Per Diem | **(B)** Estimated Level of Effort (LOE) for (A) (Working Days) | **(C)**<br>**Sub-total (AxB)** | **(D)**<br>Option Periods Firm all-inclusive Per Diem | **(E)** Estimated LOE for (D) (Working Days) | **(F)**<br>**Sub-total (DxE)** | **(G)**<br>**Total Estimated Cost per Resource Category**<br>**[C+F]** |
| 1.Communications Consultant (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 2.Courseware Developer (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 3.Data Conversion Specialist (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |
| 4.Database Administrator (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |
| 5.Database Modeller / IM Modeler (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |

| TABLE 2 | **AS-AND-WHEN-REQUESTED WORK (Section 9 of ANNEX A - SOW) – TASK AUTHORIZATIONS – Resource Categories *(for financial evaluation)*** | | | | | | |
|---|---|---|---|---|---|---|---|
| **Resource Categories** | **(A)**<br>Initial Contract Period Firm All-Inclusive Per Diem | **(B)** Estimated Level of Effort (LOE) for (A) (Working Days) | **(C)**<br>**Sub-total (AxB)** | **(D)**<br>Option Periods Firm all-inclusive Per Diem | **(E)** Estimated LOE for (D) (Working Days) | **(F)**<br>**Sub-total (DxE)** | **(G)**<br>**Total Estimated Cost per Resource Category**<br>**[C+F]** |
| 6.Information Management Architect (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |
| 7.Programmer / Analyst – Business Objects (Level 3) | $0.00 | 120 | $0.00 | $0.00 | 120 | $0.00 | $0.00 |
| | | | | | | | |
| 8.Programmer / Analyst - MS Dynamics CRM (Level 3) | $0.00 | 120 | $0.00 | $0.00 | 120 | $0.00 | $0.00 |
| | | | | | | | |
| 9.Web Developer (Level 3) | $0.00 | 120 | $0.00 | $0.00 | 120 | $0.00 | $0.00 |
| | | | | | | | |
| 10.Business Process Re-engineering (BPR) Consultant (Level | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |
| 11.Change Management Consultant (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 12.Cybersecurity Specialist (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |
| 13.Incident Management Specialist (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 14.IT Security Design Specialist (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 15.IT Security Engineer (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 16.IT Security VA Specialist (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 17.Network Analyst (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |
| 18.Operations Support Specialist (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 19.System Auditor (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 20.Testing Coordinator (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 21.Web Designer (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 22.Programmer / Software Developer (Level 3) | $0.00 | 120 | $0.00 | $0.00 | 120 | $0.00 | $0.00 |
| | | | | | | | |

| TABLE 2 | **AS-AND-WHEN-REQUESTED WORK (Section 9 of ANNEX A - SOW) – TASK AUTHORIZATIONS – Resource Categories *(for financial evaluation)*** | | | | | | |
|---|---|---|---|---|---|---|---|
| **Resource Categories** | **(A)**<br>Initial Contract Period Firm All-Inclusive Per Diem | **(B)** Estimated Level of Effort (LOE) for (A) (Working Days) | **(C)**<br>**Sub-total (AxB)** | **(D)**<br>Option Periods Firm all-inclusive Per Diem | **(E)** Estimated LOE for (D) (Working Days) | **(F)**<br>**Sub-total (DxE)** | **(G)**<br>**Total Estimated Cost per Resource Category**<br>**[C+F]** |
| 23.Application/Software Architect (Level 3) | $0.00 | 40 | $0.00 | $0.00 | 80 | $0.00 | $0.00 |
| | | | | | | | |
| 24.Database Analyst (Level 3) | $0.00 | 80 | $0.00 | $0.00 | 40 | $0.00 | $0.00 |
| | | | | | | | |

| | |
|---|---|
| **(H) Total Cost [Sum of (G) for all Resource Categories]** | **$0.00** |

**4. <u>Total Evaluated Bid Price:</u>**

| | |
|---|---|
| The Total Evaluated Bid Price will be calculated as follows: | |
| **Actual Total Evaluated Bid Price:** | **$0.00** |

Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

*Better government: with partners, for Canadians*

# Cyber Authentication Technology Solutions Interface Architecture and Specification Version 2.0: Deployment Profile

**Status: Draft r8.0**
**Date modified: 16 February, 2012 14:14**
File name: TBSSCT-#1045218-v4-CA_-_CATS_IA&S_V2_0_Deployment_Profile_Draft_r8_0_en.DOC

**For further information contact:**
**Bob Sunday**
**Cyber-Authentication Initiative**
**Chief Information Officer Branch**
**Treasury Board Secretariat**
**613-941-4764**
**Email: robert.sunday@tbs-sct.gc.ca**

| | |
|---|---|
| **Approved by:** | TBS, DCIO |
| | Cyber-Auth DG Committee |

## Revision Record Sheet

| VERSION NO. | DESCRIPTION | DATE ISSUED | Status | AUTHOR & NOTES |
|---|---|---|---|---|
| Draft r8.0 | Initial text with marked changes based on CA - CATS IA&S V2.0_Deployment Profile_Final r7.2_en.doc | 16 February 2012 | Draft to incorporate GCCF decisions | Bob Sunday, TBS |
| | | | | |

### Release Note for this version Draft r8.0

This “*Cyber Authentication Technology Solutions - Interface Architecture and Specification - Version 2.0: Deployment Profile*” is an updated draft of the baseline document: <<CA - CATS IA&S V2.0_Deployment Profile_Final r7.2_en.doc>>. This release contains approved GCCF architectural changes to the official baseline document and some minor editorial enhancements.

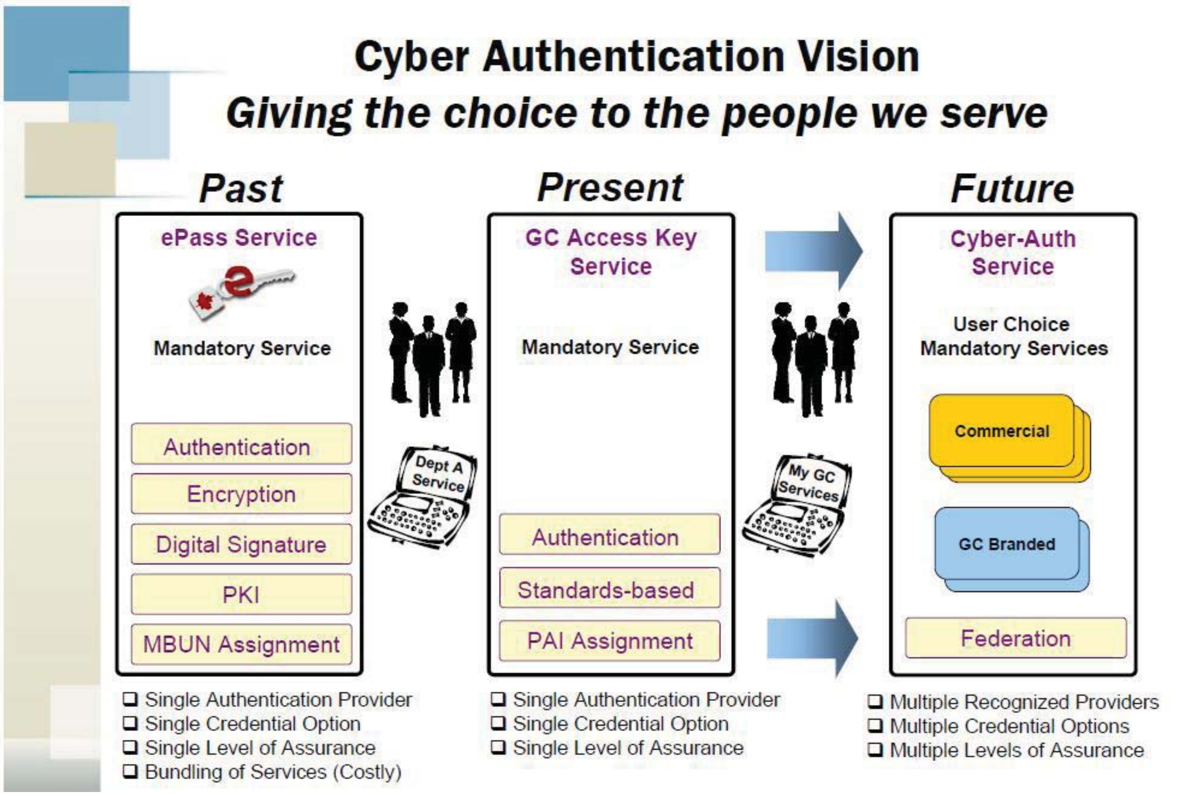
Subsequent changes to this baseline document will be processed with official change requests and dispositions.

# Table of Contents

# 1 Introduction

## 1.1 The Cyber Authentication Initiative Vision

The Cyber Authentication Initiative at the Government of Canada has a Vision which is partially described in the following diagram:



Cyber Authentication Vision
Giving the choice to the people we serve
Past
ePass Service
Mandatory Service
Authentication
Encryption
Digital Signature
PKI
MBUN Assignment
Dept A Service
Present
GC Access Key Service
Mandatory Service
Authentication
Standards-based
PAI Assignment
My GC Services
Future
Cyber-Auth Service
User Choice
Mandatory Services
Commercial
GC Branded
Federation
❑ Single Authentication Provider
❑ Single Credential Option
❑ Single Level of Assurance
❑ Bundling of Services (Costly)
❑ Single Authentication Provider
❑ Single Credential Option
❑ Single Level of Assurance
❑ Multiple Recognized Providers
❑ Multiple Credential Options
❑ Multiple Levels of Assurance

Figure 1: Cyber-Auth Vision

## 1.2 Overview of the CATS2 IA&S Deployment Profile

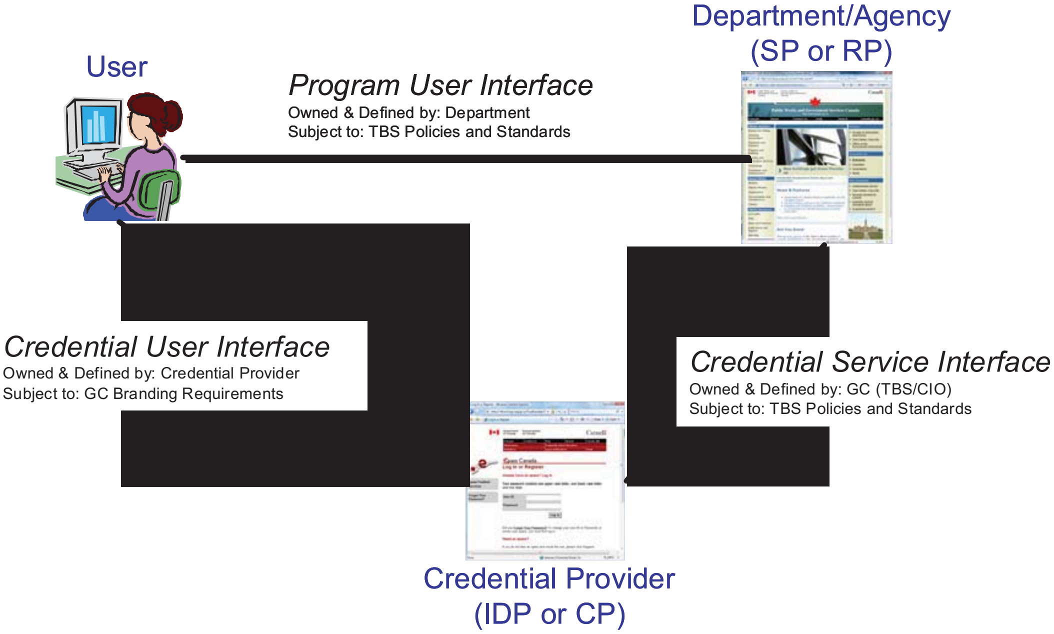

Department/Agency
(SP or RP)
User
Program User Interface
Owned & Defined by: Department
Subject to: TBS Policies and Standards
Credential User Interface
Owned & Defined by: Credential Provider
Subject to: GC Branding Requirements
Credential Service Interface
Owned & Defined by: GC (TBS/CIO)
Subject to: TBS Policies and Standards
Credential Provider
(IDP or CP)

**Figure 2: Business View of Authentication Interfaces**

This "*CATS2 IA&S Deployment Profile"* [CATS2 IA&S] is a deployment level profile for participation in the Government of Canada's Cyber-Auth environment. It describes the messaging interface referred to as the Credential Service Interface in Figure 2: Business View of Authentication Interfaces. The other interfaces shown in the diagram are defined by either the Department/Agency or the Credential Provider.

It applies to deployments configured to participate as both Service Providers (SPs) and Identity Providers (IDPs). In the current GC context, SPs are also called Relying Parties (RPs), typically departmental online services, and IDPs are called Credential Providers (CPs) or Credential Service Providers (CSPs). The GC also refers to a Credential Broker Service (CBS) which is a system entity that acts as both an IDP for RPs and as an RP when it communicates with underlying IDPs; SAML documents refer to this as a Proxying Identity Provider

*NOTE: In this document we use the terminology of SP and IDP. Other Cyber-Auth documents may use the terms RP, CP and CSP. SAML and Kantara Initiative documentation use the terms SP and IDP. This document does not use the term CBS as it is a composite implementation of the SP and IDP roles.*

*This document also uses the terms "User", Principal" and "Subject" as synonymous terms.*

This deployment profile is an evolution of the former GC document "*Cyber-Auth Tactical Solution (CATS) Interface Architecture and Specification*" [CATS1 IA&S] and is an update to the Final r7.2 version of [CATS2 IA&S].

This deployment profile is not a tutorial or guidance document. Further guidance and use cases may be provided by the Government of Canada Credential Federation (GCCF).

## 1.3 Compliance to CATS2 IA&S Deployment Profile

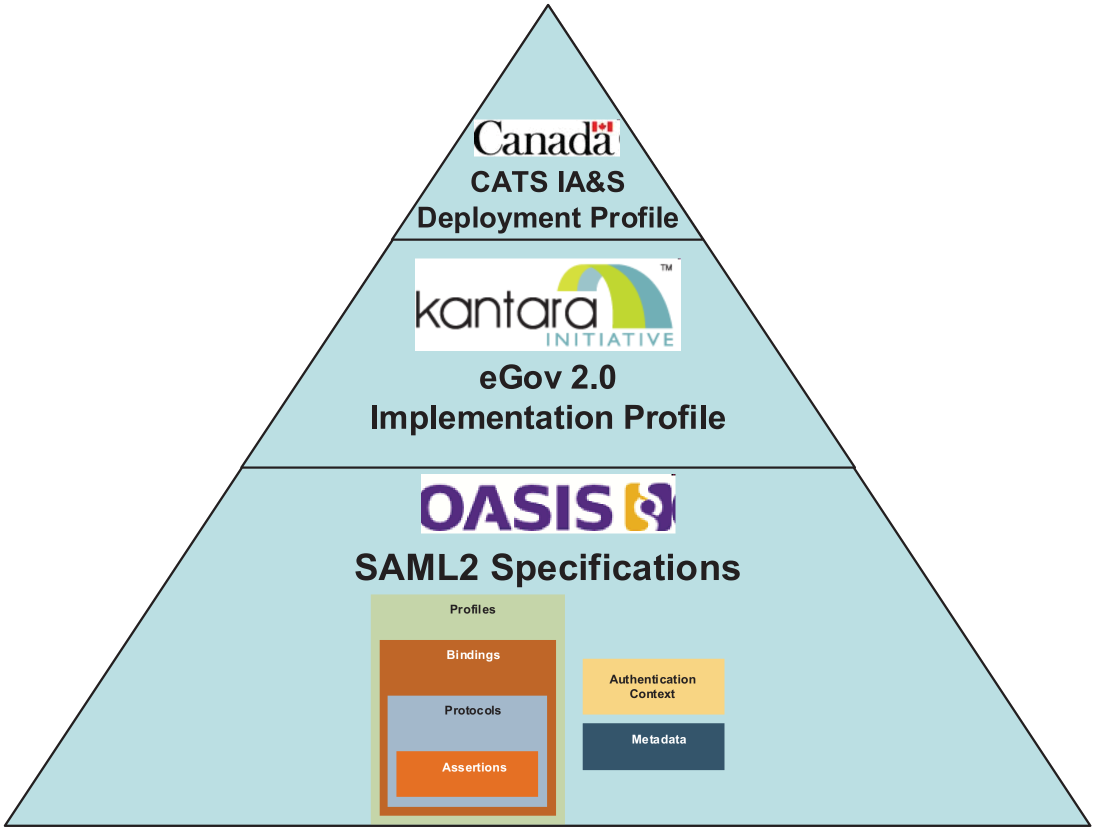


**Figure 3: The Cyber-Auth Interface Architecture Building Blocks**

This deployment profile is based on but does not require full compliance with the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative. The normative requirements of this GC Deployment Profile in terms of the applicable sections of the eGov 2.0 Profile are detailed in Section 2 of this document. The eGov 2.0 Profile is based on the SAML 2.0 specifications created by the Security Services Technical Committee (SSTC) of OASIS. The eGov 2.0 Profile constrains the base SAML 2.0 features, elements, attributes and other values required for approved eGovernment federations and deployments. Unless otherwise specified, SAML operations and features follow those found in the OASIS SAML 2.0 specifications [SAML2 *].

*NOTE: Interoperability testing conducted by external bodies, such as the Kantara Initiative, may assist confirmation of compliance. As such, GC acquisitions which require compliance with this deployment profile may also require the underlying software to comply with external interoperability testing.*

*However, these external tests do not form a complete and final confirmation of compliance with these GC deployment requirements. Additional testing may be required by the GC Credential Federation (GCCF) to allow participation in the GCCF.*

### 1.3.1 Notation

This specification uses normative text to describe the use of SAML capabilities.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC2119]:

> …they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)…

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations.

## 1.4 Changes from the previous CATS2 document, *Final r7.2*

This document, [CATS2 IA&S r8], differs from the [CATS2 IA&S r7.2] in a number of areas:

These changes are generally described below; the full detailed normative conformance requirements for this deployment profile are specified within this document in Section 2 titled: “Deployment Requirements (Normative)”

### 1.4.1 A template for GCCF Value Assignment

An Appendix has been added to provide a template for all the CATS2 values which must be assigned by the GCCF Operator. This includes:

- LoAs
- SPNameQualifier
- SessionNotOnOrAfter
- Common Domain Name

### 1.4.2 GCCF Decisions

**GCCF-0001: IDP Discovery Cookie**

The intention of CATS2 was to make the Identity Provider Discovery Profile mandatory for all IDPs and optional for SPs. There is one statement in the normative section of CATS2 (Section 2.1, eGov 2.5.1) that could cause some confusion and this change clarifies it.

**GCCF-0003: ICM SSL Certs**

This removes the requirement that Federation Members use ICM SSL certificates when using SOAP over TLS to transport messages in section 2.4.5.4.2

**GCCF-0006: Levels of Assurance Values**

This moves the assignment of Level of Assurance values to the GCCF operator.

**GCCF-0008: GC Language Cookie**

This changes the Language values from “en” and “fr” to “eng” and “fra”.

### 1.4.3 A Number of Miscellaneous Corrections/Updates

A number of miscellaneous corrections/updates were required:

- The vision diagram was updated.
- GCCFGB was updated to GCCF everywhere
- A correction to IDP Metadata removes the need to have a < ManageNameIDService> SOAP end point

## 1.5 Document References

[CATS1 IA&S] “Cyber-Auth Tactical Solution Interface Architecture and Specification Version 1.0” dated 23 January, 2009

[CATS2 IA&S r7.2] “*Cyber-Auth Technology Solutions Interface Architecture and Specification Version 2.0: Deployment Profile*” Final r7.2, published on 25 March, 2011.

[CATS2 IA&S r8.0] This document “*Cyber-Auth Technology Solutions Interface Architecture and Specification Version 2.0: Deployment Profile*” Draft r8.0

[eGov 2.0] “Kantara Initiative eGovernment Implementation Profile of SAML V2.0 Version 2.0” available from http://kantarainitiative.org/confluence/download/attachments/42139782/kantara-egov-saml2-profile-2.0.pdf

[GCCF Glossary] to be produced by GCCF
Interim definitions are available on GCPedia at
http://www.gcpedia.gc.ca/wiki/GC_Credential_Federation/Glossary

[GCCF Values] to be completed by GCCF Operator

[ISO 639-2/T] ISO 639-2:1998(E/F), “Codes for the representation of names of languages — Part 2: Alpha-3 code”
available from the Standards Council of Canada (http://www.scc.ca)

[ITSA-11] “CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within the Government of Canada”
published by Communications Security Establishment Canada and available from
http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/index-eng.html

[ITSG-31] "IT Security Guidance: User Authentication Guidance for IT Systems" published by Communications Security Establishment Canada and available from http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels http://www.ietf.org/rfc/rfc2119.txt

[SAML2 *] All the SAML2 document references are available at http://docs.oasis-open.org/security/saml/v2.0 or alternatively at http://wiki.oasis-open.org/security/FrontPage

[SAML2 Assur] OASIS Committee Specification 01, SAML V2.0 Identity Assurance Profiles Version 1.0, November 2010. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf

[SAML2 Bind] OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML2 Core] OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2 Errata] OASIS SAML V2.0 Approved Errata, 1 December 2009. http://www.oasis-open.org/committees/download.php/37166/sstc-saml-approved-errata-2.0-02.pdf

[SAML2 Meta] OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2 MetaUI] OASIS Working Draft 06, Metadata Extensions for Login and Discovery User Interface Version 1.0, November 2010 http://www.oasis-open.org/committees/download.php/40270/sstc-saml-metadata-ui-v1.0-wd06.pdf

[SAML2 Prof] OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

# 2 Deployment Requirements (Normative)

## 2.1 Constraints on the Kantara Initiative eGov 2.0 Profile

This specification builds upon the SAML 2.0 suite of specifications [SAML2 *] and the profile of SAML2 referred to as Kantara Initiative eGovernment Implementation Profile of SAML2 version 2.0 [eGov 2.0]

This deployment profile is based on but does not require full compliance with the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative (see the note in Section 1.3 on page 5). While the Kantara eGov 2.0 profile is an “implementation” profile for vendors of software products, this Cyber-Auth profile is a “deployment” profile which further constrains and explains the deployment of SPs and IDPs in the GC Cyber-Auth environment. Where this *“CATS2 IA&S Deployment Profile”* does not explicitly provide SAML2 guidance, one MUST implement in accordance with applicable OASIS SAML 2.0 requirements

The following table is in the order and description of the requirements in [eGov 2.0], Sections 2 & 3 which are repeated word for word in the first column. The table is annotated with the support required by the GC Cyber-Auth Initiative: typically this is either “Support” or “Constrained” or “n/a” (not applicable). Whenever further details are required to fully explain the GC requirement, they are provided in the 3rd column.

There are also requirements which are additional to these eGov 2.0 requirements and they are specified in the subsequent sections. Cyber-Auth also has constraints on the SAML v2.0 specifications and has a few Cyber-Auth specific requirements

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| eGov 2.2 Metadata and Trust Management | | |
| Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections. Additional expectations around the use of particular metadata elements related to profile behavior may be encountered in those sections. | Support | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| eGov 2.2.1 Metadata Profiles | | |
| Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP]. | Constrained | Cyber-Auth Deployments MUST NOT use the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP]. |
| In addition, implementations MUST support the use of the <md:KeyDescriptor> element as follows: | Support | |
| • Implementations MUST support the <ds:X509Certificate> element as input to subsequent requirements. Support for other key representations, and for other mechanisms for credential distribution, is OPTIONAL. | Constrained | No OPTIONAL mechanisms are supported |
| • Implementations MUST support some form of path validation of signing, TLS, and encryption credentials used to secure SAML exchanges against one or more trusted certificate authorities. Support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280]. | Support | Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.5 Security |
| • Implementations MUST support the use of OCSP [RFC2560] and Certificate Revocation Lists (CRLs) obtained via the "CRL Distribution Point" X.509 extension [RFC5280] for revocation checking of those credentials. | Constrained | Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.5 Security |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| • Implementations MAY support additional constraints on the contents of certificates used by particular entities, such as "subjectAltName" or "DN", key usage constraints, or policy extensions, but SHOULD document such features and make them optional to enable where possible. | Constrained | No OPTIONAL additional constraints are supported |
| Note that these metadata profiles are intended to be mutually exclusive within a given deployment context; they are alternatives, rather than complimentary or compatible uses of the same metadata information. | n/a | |
| Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism. | Support | |
| eGov 2.2.2 Metadata Exchange | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| It is OPTIONAL for implementations to support the generation or exportation of metadata, but implementations MUST support the publication of metadata using the Well-Known-Location method defined in section 4.1 of [SAML2 Meta] (under the assumption that entityID values used are suitable for such support). | Constrained | The GC Credential Federation maintains and distributes current metadata. To terminate Federation member use of non-current metadata, the GCCF stops distributing it. In addition, the GCCF may revoke a certificate in the metadata file for reasons including, but not limited to terminating a Federation member’s participation, certificate compromise, and key changes.<br>• Federation members MUST submit the XML metadata document to the GCCF.<br>• Federation members MUST only accept XML metadata documents from the GCCF. |
| Implementations MUST support the following mechanisms for the importation of metadata:<br>• local file<br>• remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL [RFC2818]<br>In the case of HTTP resolution, implementations MUST support use of the "ETag" and "Last-Modified" headers for cache management. Implementations SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a single entity's metadata is present in more than one source. | Constrained | The GC Credential Federation maintains and distributes current metadata as specified above. Any additional procedures will be established by the GCCF |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element MUST be supported. | Constrained | Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element SHOULD be supported.<br>• The GC Credential Federation maintains and distributes current metadata. If necessary, this distribution may be modified to allow vendor software that does not support Importation of multiple entities' metadata contained within an <md:EntitiesDescriptor> element |
| Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without service degradation or interruption. | Support | |
| eGov 2.2.2.1 Metadata Verification | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Verification of metadata, if supported, MUST include XML signature verification at least at the root element level, and SHOULD support the following mechanisms for signature key trust establishment:<br>• Direct comparison against known keys.<br>• Some form of path-based certificate validation against one or more trusted certificate authorities, along with certificate revocation lists and/or OCSP [RFC2560]. Support for PKIX [RFC5280] is RECOMMENDED; implementations SHOULD document the behavior of the validation mechanisms they employ, particular with respect to limitations or divergence from PKIX [RFC5280]. | Constrained | • Federation members MUST sign their metadata using the signing certificate issued by the GC ICM Service.<br>• At consumption time, the Federation member relying upon the metadata MUST check the revocation status of the certificate used to sign the metadata.<br>○ Only CRL's are supported |
| eGov 2.3 Name Identifiers | | |
| In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:<br>• urn:oasis:names:tc:SAML:2.0:nameid-format:persistent<br>• urn:oasis:names:tc:SAML:2.0:nameid-format:transient | Constrained | Cyber-Auth Deployments MUST support persistent<br>Cyber-AuthDeployments MUST NOT support transient |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Support for other formats is OPTIONAL. | Constrained | Cyber-AuthDeployments MUST NOT support other formats |
| eGov 2.4 Attributes | | |
| In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity Provider and Service Provider implementations MUST support the generation and consumption of <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500]. | Constrained | Cyber-AuthDeployments MUST follow the requirements specified in Section 2.4.1 Required Assertion Attributes |
| The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g., <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an alternative. | Constrained | Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.1 Required Assertion Attributes |
| eGov 2.5 Browser Single Sign-On | | |
| This section defines an implementation profile of the SAML V2.0 Web Browser SSO Profile [SAML2Prof]. | Support | |
| eGov 2.5.1 Identity Provider Discovery | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IDPDisco]. | Constrained | Cyber-Auth IDP Deployments MUST support the Identity Provider Discovery specified in [SAML2 Prof]<br>Cyber-Auth SP Deployments MAY support the Identity Provider Discovery specified in [SAML2 Prof]<br>Cyber-Auth Deployments MUST NOT support the Identity Provider Discovery Service protocol Profile specified in [SAML2 Disco] |
| eGov 2.5.2 Authentication Requests | | |
| eGov 2.5.2.1 Binding and Security Requirements | | |
| Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the generation or verification of signatures in conjunction with this binding. | Support | |
| Support for other bindings is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST NOT support other bindings |
| eGov 2.5.2.2 Message Content | | |
| In addition to standard core- and profile-driven requirements, Service Provider implementations MUST support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes (when appropriate): | Constrained | As specified below |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| • AssertionConsumerServiceURL | Constrained | Cyber-Auth Deployments SHOULD NOT use AssertionConsumerServiceURL<br>• The IDP will obtain this from the metadata |
| • ProtocolBinding | Constrained | If present, ProtocolBinding attribute MUST be urn:oasis:names:tc:SAML:2.0:bindings: HTTP-POST. |
| • ForceAuthn | Constrained | ForceAuthn MAY be used to require the IDP to force the end user to authenticate to the IDP regardless of the end user's authentication session status at the IDP.<br>• When ForceAuthn is used, the IDP MUST ensure that the principal does not change their NameID from any previous authentication in this session even if it has expired.<br>• if ForceAuthn is used and the authentication is successful, this will reset the IDPs AuthnInstant for this principal. |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| • IsPassive | Constrained | • IsPassive MAY be used if the SP does not wish for the IDP to take direct control of the end user’s browser (i.e., show the end user a page).<br>• If IsPassive is true, the end user MUST be able to authenticate in some passive manner, otherwise the resulting response MUST NOT contain an <Assertion>.<br>• This feature allows the SP to determine whether it should alert the end user that he or she is about to interact with the IDP. An example of a passive situation is: the SP discovers through the common domain cookie that the end user may have an active session at a particular IDP. |
| • AttributeConsumingServiceIndex | Constrained | Cyber-Auth Deployments MUST NOT specify AttributeConsumingServiceIndex. |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| • <saml2p:RequestedAuthnContext> | Constrained | • The authentication request MUST include <RequestedAuthnContext><br>• The <RequestedAuthnContext> MUST include a Level of Assurance as specified in [SAML2 Assur]. The GC Cyber-Auth LoA's are defined in Section 2.4.2 GC Cyber-Auth Levels of Assurance.<br>• SPs MUST request a specific level of assurance with the "exact" comparison operator.<br>• The SP MAY request more than one level of assurance in priority order. E.g. this is useful when a level 2 is required but the SP is willing to accept a level 3 if a level 2 is not possible. |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| • <saml2p:NameIDPolicy> | Constrained | • <SPNameQualifier> MAY be present<br>○ The GCCF may establish affiliation groups of GCCF SPs that will use a common Persistent Anonymous Identifier. In this case SPs MAY use the <SPNameQualifier> in the Authentication Request to indicate their desire for this common PAI.<br>• <NameIDPolicy> MAY contain AllowCreate attribute.<br>○ In general, AllowCreate will be set to true so that if the end user has never used the selected IDP to access the SP, an end user identifier can be created, and SAML messages can be exchanged between the parties.<br>○ However, AllowCreate set to false may be useful if the SP wishes to disable credential registration flows in the user interface at the IDP<br>• If Format is present it MUST be urn:oasis:names:tc:SAML:2.0:nameid-format:persistent. |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations MUST fully support the options enumerated above, and be configurable to utilize those options in a useful manner as defined by [SAML2Core]. | Support | |
| Implementations MAY limit their support of the <saml2p:RequestedAuthnContext> element to the value "exact" for the Comparison attribute, but MUST otherwise support any allowable content of the element. | Constrained | Cyber-Auth Deployments MUST only support “exact” for the Comparison attribute. |
| Identity Provider implementations MUST support verification of requested AssertionConsumerServiceURL locations via comparison to <md:AssertionConsumerService> elements supplied via metadata using case-sensitive string comparison. It is OPTIONAL to support other means of comparison (e.g., canonicalization or other manipulation of URL values) or alternatve verification mechanisms. | Constrained | Cyber-Auth Deployments MUST NOT support other means of comparison |
| eGov 2.5.3 Responses | | |
| eGov 2.5.3.1 Binding and Security Requirements | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST and HTTP-Artifact bindings [SAML2Bind] for the transmission of <saml2p:Response> messages. | Constrained | Cyber-Auth Deployments MUST support HTTP POST bindings<br>Cyber-Auth Deployments MUST NOT support HTTP Artifact bindings |
| Support for other bindings, and for artifact types other than urn:oasis:names:tc:SAML:2.0:artifact-04, is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST NOT support other bindings |
| Identity Provider and Service Provider implementations MUST support the generation and consumption of unsolicited <saml2p:Response> messages (i.e., responses that are not the result of a <saml2p:AuthnRequest> message). | Constrained | Cyber-Auth Deployments MUST discard unsolicited <saml2p:Response> messages<br>● No Cyber-Auth use case has been identified which requires these |
| Identity Provider implementations MUST support the issuance of <saml2p:Response> messages (with appropriate status codes) in the event of an error condition, provided that the user agent remains available and an acceptable location to which to deliver the response is available. The criteria for "acceptability" of a response location are not formally specified, but are subject to Identity Provider policy and reflect its responsibility to protect users from being sent to untrusted or possibly malicious parties. Note that this is a stronger requirement than the comparable language in [SAML2Prof]. | Support | The GCCF defines “acceptability of a response location” to mean the metadata registered <AssertionConsumerServiceURL> |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Identity Provider and Service Provider implementations MUST support the signing of <saml2:Assertion> elements in responses; support for signing of the <saml2p:Response> element is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST NOT support signing of the <saml2p:Response> element |
| Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedAssertion> element when using the HTTP-POST binding; support for the <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST NOT deploy OPTIONAL support |
| eGov 2.5.3.2 Message Content | | |
| The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of <saml2:Assertion>, <saml2:AuthnStatement>, and <saml2:AttributeStatement> elements in the <saml2p:Response> message to be limited to one. In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing <saml2p:Response> messages. | Constrained | Cyber-Auth Deployments MUST only send <saml2p:Response> messages containing at most a single <saml2:Assertion> |
| Identity Provider implementations MUST support the inclusion of a Consent attribute in <saml2p:Response> messages, and a SessionIndex attribute in <saml2:AuthnStatement> elements. | Constrained | Cyber-Auth IDP Deployments MUST NOT include a Consent attribute in <saml2p:Response> messages<br>• No Cyber-Auth use case has been identified which requires this. |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Service Provider implementations that provide some form of session semantics MUST support the <saml2:AuthnStatement> element's SessionNotOnOrAfter attribute. | Support | See section 2.2 for constraints on Cyber-Auth IDP deployments |
| Service Provider implementations MUST support the acceptance/rejection of assertions based on the content of the <saml2:AuthnStatement> element's <saml2:AuthnContext> element. Implementations also MUST support the acceptance/rejection of particular <saml2:AuthnContext> content based on the identity of the Identity Provider. [IAP] provides one such mechanism via SAML V2.0 metadata and is RECOMMENDED; though this specification is in draft form, the technical details are not expected to change prior to eventual approval. | Support | |
| eGov 2.5.4 Artifact Resolution | | |
| Pursuant to the requirement in section 2.5.3.1 for support of the HTTP-Artifact binding [SAML2Bind] for the transmission of <saml2p:Response> messages, implementations MUST support the SAML V2.0 Artifact Resolution profile [SAML2Prof] as constrained by the following subsections. | Constrained | Cyber-Auth deployments MUST NOT support the HTTP-Artifact binding |
| eGov 2.5.4.1 Artifact Resolution Requests | | |
| Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResolve> messages. | n/a | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate requests; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL. | n/a | |
| eGov 2.5.4.2 Artifact Resolution Responses | | |
| Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResponse> messages. | n/a | |
| Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate responses; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL. | n/a | |
| eGov 2.6 Browser Holder of Key Single Sign-On | | |
| This section defines an implementation profile of the SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0 [HoKSSO]. | Constrained | Cyber-Auth Deployments MUST NOT support |
| The implementation requirements defined in section 2.5 for the non-holder-of-key profile apply to implementations of this profile. | n/a | |
| eGov 2.7 SAML 2.0 Proxying | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Section 3.4.1.5 of [SAML2Core] defines a formalized approach to proxying the SAML 2.0 Authentication Request protocol between multiple Identity Providers. This section defines an implementation profile for this behavior suitable for composition with the Single Sign-On profiles defined in sections 2.5 and 2.6. | Support | Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP |
| The requirements of the profile are imposed on Identity Provider implementations acting as a proxy. These requirements are in addition to the technical requirements outlined in section 3.4.1.5.1 of [SAML2Core], which also MUST be supported. | Support | Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP |
| eGov 2.7.1 Authentication Requests | | |
| Proxying Identity Provider implementations MUST support the mapping of incoming to outgoing <saml2p:RequestedAuthnContext> and <saml2p:NameIDPolicy> elements, such that deployers may choose to pass through values or map between different vocabularies as required. | Support | Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP |
| Proxying Identity Provider implementations MUST support the suppression/eliding of <saml2p:RequesterID> elements from outgoing <saml2p:AuthnRequest> messages to allow for hiding the identity of the Service Provider from proxied Identity Providers. | Support | Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP |
| eGov 2.7.2 Responses | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Proxying Identity Provider implementations MUST support the mapping of incoming to outgoing <saml2:AuthnContext> elements, such that deployers may choose to pass through values or map between different vocabularies as required. | Support | Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP |
| Proxying Identity Provider implementations MUST support the suppression of <saml2:AuthenticatingAuthority> elements from outgoing <saml2:AuthnContext> elements to allow for hiding the identity of the proxied Identity Provider from Service Providers. | Support | Cyber-Auth Deployments MUST support when configured to operate as a Proxying IDP |
| eGov 2.8 Single Logout | | |
| This section defines an implementation profile of the SAML V2.0 Single Logout Profile [SAML2Prof].<br>For clarification, the technical requirements for each message type below reflect the intent to normatively require initiation of logout by a Service Provider using either the front- or back-channel, and initiation/propagation of logout by an Identity Provider using the back-channel. | Support | |
| eGov 2.8.1 Logout Requests | | |
| eGov 2.8.1.1 Binding and Security Requirements | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the issuance of <saml2p:LogoutRequest> messages, and MUST support the SAML SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the reception of <saml2p:LogoutRequest> messages. | Support | |
| Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for both issuance and reception of <saml2p:LogoutRequest> messages. | Support | |
| Support for other bindings is OPTIONAL. | Constrained | Cyber-Auth SP deployments MAY support HTTP Redirect bindings for issuance of <saml2p:LogoutRequest> messages<br>No other bindings are supported |
| Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate <saml2p:LogoutRequest> messages; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST follow the requirements specified in Section 2.4.5 Security |
| Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedID> element when using the HTTP-Redirect binding. | Support | |
| eGov 2.8.1.2 User Interface Behavior | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Identity Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout. Upon receipt of a <saml2p:LogoutRequest> message via a front-channel binding, Identity Provider implementations MUST support user intervention governing the choice of propagating logout to other Service Providers, or limiting the operation to the Identity Provider. Of course, implementations MUST return status information to the requesting entity (e.g. partial logout indication) as appropriate. | Constrained | Cyber-Auth deployments MUST NOT deploy support for user intervention governing the choice of propagating logout to other SPs, or limiting the operation to the Identity Provider.<br>• At all times, a Single Logout Request will generate a global logout for the principal's session. |
| Service Provider implementations MUST support both user-initiated termination of the local session only and user-initiated Single Logout. | Constrained | Cyber-Auth SP deployments MAY only deploy support for Single Logout (i.e. global logout).<br>• Cyber-Auth IDP deployments MUST propagate the logout without user intervention to all SPs involved in the session and respond to the originating SP. |
| Identity Provider implementations MUST also support the administrative initiation of Single Logout for any active session, subject to appropriate policy. | Support | The GCCF will specify, for each Cyber-Auth IDP deployment, what, if any, support for administrative initiation of Single Logout is required. |
| eGov 2.8.2 Logout Responses | | |
| eGov 2.8.2.1 Binding and Security Requirements | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the issuance of <saml2p:LogoutResponse> messages, and MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the reception of <saml2p:LogoutResponse> messages. | Constrained | • Note: HTTP Redirect bindings for issuance of <saml2p:LogoutResponse> messages are deprecated and SHOULD ONLY be used if the <saml2p:LogoutRequest> message was sent using this binding. |
| Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2 Bind] for both issuance and reception of <saml2p:LogoutResponse> messages. | Support | |
| Support for other bindings is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST NOT deploy OPTIONAL support |
| Implementations MUST support the use of SAML message signatures and TLS server authentication to authenticate <saml2p:LogoutResponse> messages; support for TLS client authentication, or other forms of authentication in conjunction with the SAML SOAP binding, is OPTIONAL. | Constrained | Cyber-Auth Deployments MUST NOT deploy OPTIONAL support |
| eGov 3 Conformance Classes | | |
| eGov 3.1 Standard | | |
| Conforming Identity Provider and/or Service Provider implementations MUST support the normative requirements in sections 2.2, 2.3, 2.4, and 2.5. | Support | |
| eGov 3.1.1 Signature and Encryption Algorithms | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Implementations MUST support the signature and digest algorithms identified by the following URIs in conjunction with the creation and verification of XML Signatures [XMLSig]:<br>• http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (defined in [RFC4051])<br>• http://www.w3.org/2001/04/xmlenc#sha256 (defined in [XMLEnc]) | Support | This requirement extends to the algorithms used for signing  URL-encoded SAML messages as described in section 3.4.4.1 of [SAML-Bindings] |
| Implementations SHOULD support the signature and digest algorithms identified by the following URIs in conjunction with the creation and verification of XML Signatures [XMLSig]:<br>• http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 (defined in [RFC4051]) | Support | |
| Implementations MUST support the block encryption algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]:<br>• http://www.w3.org/2001/04/xmlenc#tripledes-cbc<br>• http://www.w3.org/2001/04/xmlenc#aes128-cbc<br>• http://www.w3.org/2001/04/xmlenc#aes256-cbc | Support | Algorithms used MUST be CSEC Approved Cryptographic Algorithms for Electronic Authentication and Authorization Applications  as documented in [ITSA-11]. |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Implementations MUST support the key transport algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]:<br>• http://www.w3.org/2001/04/xmlenc#rsa-1_5<br>• http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p | Support | Algorithms used MUST be CSEC Approved Cryptographic Algorithms for Electronic Authentication and Authorization Applications as documented in [ITSA-11]. |
| Implementations SHOULD support the key agreement algorithms identified by the following URIs in conjunction with the use of XML Encryption [XMLEnc]:<br>• http://www.w3.org/2009/xmlenc11#ECDH-ES defined in [XMLEnc11])<br>(This is a Last Call Working Draft of XML Encryption 1.1, and this normative requirement is contingent on W3C ratification of this specification without normative changes to this algorithm's definition.) | Support | Algorithms used MUST be CSEC Approved Cryptographic Algorithms for Electronic Authentication and Authorization Applications as documented in [ITSA-11]. |
| Support for other algorithms is OPTIONAL. | Constrained | CA Deployments MUST NOT support other algorithms. |
| eGov 3.2 Standard with Logout | | |

| eGov 2.0 | CATS IA&S Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| Conforming Identity Provider and/or Service Provider implementations MUST meet the conformance requirements in section 3.1, and MUST in addition support the normative requirements in section 2.8. | Constrained | See section 2.8 above |
| eGov 3.3 Full | | |
| Conforming Identity Provider and/or Service Provider implementations MUST meet the conformance requirements in section 3.1, and MUST in addition support the normative requirements in sections 2.6, 2.7, and 2.8. | Constrained | • Cyber-Auth deployments MUST NOT be configured to meet section 2.6<br>• Cyber-Auth deployments MUST be configured to meet section 2.7 when configured to operate as a Proxying IDP |
| End of table | | |

## 2.2 Additional Constraints on the [SAML2 *] specifications

In addition to the constraints imposed by this deployment profile on the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative, this Cyber-Auth deployment requirements document also imposes some additional constraints on the underlying SAML 2.0 specifications published by the Security Services Technical Committee (SSTC) of OASIS.

| SAML2 * | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| [SAML2 Core ]<br>Section 2.7.2, Line 1061<br>`<SessionNotOnOrAfter>` | Constrained | Cyber-Auth IDP deployments SHOULD NOT specify the SessionNotOnOrAfter attribute. This allows the SP to choose its own required duration for its security context.<br>• If a GCCF IDP is unable to configure this value to not be sent, then it MUST set this value to a high value as determined by the GCCF. |
| [SAML2 Core]<br>Section 3.2.1, Line 1489<br>`<saml:Issuer>` | Constrained | SP Authentication Request `<saml:Issuer>`<br>• MUST be present<br>• MUST be the entity_id assigned by the GCCF. |
| [SAML2 Core ]<br>Section 3.4.1, Line 2017<br>`<saml:Subject>` | Constrained | SP Authentication Request `<saml:Subject>` MUST NOT be included.<br>• no Cyber-Auth use cases require the `<saml:Subject>` element |
| [SAML2 Core ]<br>Section 3.4.1, Line 2029<br>`<saml:Conditions>` | Constrained | SP Authentication Request `<saml:Conditions>` MUST NOT be included.<br>• no Cyber-Auth use cases require the `<saml:Conditions>` element |

| SAML2 * | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| [SAML2 Core]<br>Section 3.4.1, Line 2068<br>ProtocolBinding | Constrained | SP Authentication Request ProtocolBinding<br>• MAY be used<br>• If ProtocolBinding is present it MUST be "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" |
| [SAML2 Core]<br>Section 3.6.1, Line 2421<br><ManageNameIDRequest> | Constrained | IDP deployments MUST send in a timely manner a <ManageNameIDRequest> with <Terminate> for a credential that has been revoked to any SP that has an endpoint defined for the <ManageNameIDService> and for which it has previously sent an assertion for the principal.<br>IDP deployments MUST NOT send any other <ManageNameIDRequest> messages.<br>SP deployments MUST respond to <ManageNameIDRequest> messages |
| [SAML2 Bind]<br>Section 3.5.3, Line 785<br><RelayState> | Constrained | <RelayState> MAY NOT be included in a response message unless it has been provided in a corresponding request message. |

| SAML2 * | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| [SAML2 Assur]<br>Section 3, Line 276<br>`<assurance-certification>` | Constrained | Metadata for Cyber-Auth IDPs MUST specify the supported Level(s) of Assurance in the `<assurance-certification>` attribute as defined in [SAML2 Assur], Section 3 Identity Assurance Certification Attribute Profile<br>The URI values to be used for the 4 levels of Assurance are defined in Section 2.4.2 GC Cyber-Auth Levels of Assurance.<br>Multiple LoA values MAY be specified in the IDP's Metadata but only a single value is returned in an authentication response. |
| [SAML2 Meta]<br>Section 2.3.2, Line 371<br>`<entityID>` | Constrained | `<entityID>` MUST be agreed upon by the entity and the GCCF |
| [SAML2 Meta]<br>Section 2.3.2.1, Line 443<br>`<Organization>` | Constrained | It is RECOMMENDED that `<Organization>` be present and include either `OrganizationName` or `OrganizationDisplayName`. |
| [SAML2 Meta]<br>Section 2.3.2.2, Line 476<br>`<ContactPerson>` | Constrained | `<ContactPerson>` is RECOMMENDED<br>Cyber-Auth suggests including include either EmailAddress or TelephoneNumber |
| [SAML2 Meta]<br>Section 2.4.1, Line 550<br>`<RoleDescriptor>` | Constrained | • Metadata element `<RoleDescriptor>` MUST NOT be used |

| SAML2 * | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| [SAML2 Meta]<br>Section 2.4.3, Line 683<br>`<IDPSSODescriptor>`<br>including<br>Section 2.4.2, Line 643<br>`<SSODescriptorType>` | Constrained | • `WantAuthnRequestsSigned` MUST be set to true.<br>• Exactly two instances of `<SingleLogoutService>` MUST be present (one for each of the Bindings: SOAP and HTTP Redirect)<br>• Exactly one `<SingleSignOnService>` MUST be present. |
| [SAML2 Meta]<br>Section 2.4.4, Line 736<br>`<SPSSODescriptor>`<br>including<br>Section 2.4.2, Line 643<br>`<SSODescriptorType>` | Constrained | • `AuthnRequestsSigned` MUST be set to true.<br>• `WantAssertionsSigned` MUST be set to true.<br>• `<AssertionConsumerService>` MUST be included<br>• Exactly one `<AssertionConsumerService>` MUST have the Binding set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.<br>• Exactly one < `ManageNameIDService`> MAY be present to communicate the desire to receive NameID termination messages from IDPs. The binding MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:SOAP. |
| [SAML2 Meta]<br>Section 2.4.5, Line 828<br>`<AuthnAuthorityDescriptor>` | Constrained | `<AuthnAuthorityDescriptor>` MUST NOT be used |

| SAML2 * | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| [SAML2 Meta]<br>Section 2.4.6, Line 861<br><PDPDescriptor> | Constrained | <PDPDescriptor> MUST NOT be used |
| [SAML2 Meta]<br>Section 2.5, Line 938<br><AffiliationDescriptor> | Constrained | <AffiliationDescriptor> MAY be used<br>• The GCCF may establish affiliation groups of GCCF SPs that will use a common Persistent Anonymous Identifier. In this case the GCCF will supply metadata defining these groups. |
| [SAML2 MetaUI]<br>Section 2.1.1<br><md:UIInfo> | Support | SP metadata MAY include the elements <mdui:DisplayName> and <mdui:Logo><br>The IDP MAY use these metadata elements to inform the user about the entity requesting an authentication during the associated authentication dialogue. |
| End of table | | |

## 2.3 Additional Extensions relative to the [SAML2 *] specifications

In addition to the constraints imposed by this deployment profile on the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative, this Cyber-Auth deployment requirements document also extends the underlying SAML 2.0 specifications published by the Security Services Technical Committee (SSTC) of OASIS.

| SAML2 * | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| None defined | | |
| End of table | | |

## 2.4 Other GC Requirements

In addition to the constraints imposed by this deployment profile on the eGov 2.0 Profile [eGov 2.0] published by the Kantara Initiative, and the additional constraints and extensions on the underlying SAML 2.0 specifications published by the Security Services Technical Committee (SSTC) of OASIS, this Cyber-Auth Deployment Requirements document also imposes some additional requirements for the GC's Cyber-Auth environment.

### 2.4.1 Required Assertion Attributes

| Cyber-Auth Requirement | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| [SAML2 Core]<br>Section 2.7.3, Line 1165<br>`<AttributeStatement>` | Extended | Cyber-Auth SP and IDP Deployments MUST support Cyber-Auth mandatory attributes:<br>• As defined in 2.4.1.1 Mandatory Attributes |
| [SAML2 Core]<br>Section 2.7.3, Line 1165<br>`<AttributeStatement>` | Extended | Cyber-Auth IDP Deployments MAY support Cyber-Auth optional attributes:<br>• As defined in 2.4.1.2 Optional Attributes |
| [SAML2 Core]<br>Section 2.7.3, Line 1165<br>`<AttributeStatement>` | Constrained | Cyber-Auth SP Deployments SHALL NOT support receiving any other attributes<br>• A Cyber-Auth SP Deployment MUST discard any other attributes and not use the attribute values for any processing. |

| Cyber-Auth Requirement | CATS IA&S<br>Support Required | Cyber-Auth Deployment Details |
|---|---|---|
| End of table | | |

### 2.4.1.1 Mandatory Attributes

| Name (URI) | Description | Format | Datatype |
|---|---|---|---|
| ca:gc:cyber-authentication:basic:specVer | The version of the interface specification | MUST be “2.0” for this interface specification [CATS2 IA&S] | xs:string |
| End of table | | | |

### 2.4.1.2 Optional Attributes

| Name (URI) | Description | Format | Datatype |
|---|---|---|---|
| ca:gc:cyber-authentication:basic:assuranceLevel | Deprecated:<br>only included for transition from version 1 of [CATS1 IA&S]<br>The confidence level of the end authentication mechanism | MUST be one of 1, 2, 3, 4, or test | xs:string |

| Name (URI) | Description | Format | Datatype |
|---|---|---|---|
| urn:oid: 2.16.840.1.113730.3.1.39 | Deprecated:<br>only included for transition from version 1 of [CATS1 IA&S]<br>The end user's preferred language<br>(it is expected that this will be set when the end user changes their language preference during interaction with the IDP) | MUST conform to the definition of the Accept-Language header field defined in  [RFC2068] with one exception:<br>the sequence "Accept-Language" ":"<br># should be omitted. | xs:string |
| End of table | | | |

### 2.4.2 GC Cyber-Auth Levels of Assurance

Authentication Requests and Responses for the GC Cyber-Auth credentials will carry the required GC Level of Assurance. There are 4 Levels of Assurance that are defined in [ITSG-31] and used by the GC Cyber-Auth Initiative. The URI's representing these GC LoAs have values which are defined by the GCCF Operator in the [GCCF Values]. The template for these values is provided in Appendix B: B.1.1 Levels of Assurance (LoAs). Note that multiple values may be defined for each LoA.

### 2.4.3 Communicating Language Preferences

To meet the GC's Policy requirements, a method was required to send the user's (not the browser's) current language preference from the SP to the IDP and from the IDP to the SP in all cases, even when authentication fails and an assertion is not produced. Cyber-Auth will do this by utilizing a session cookie in a Common Domain defined by the GCCF (which may be the same domain established for the IDP Discovery Profile).

This session cookie will carry the language attribute, the values of which are defined in [RFC 1766]. Acceptable values for the Cyber-Auth language attribute include:

- en
- fr

Both SPs and IDPs MUST read this cookie and use this language setting in any user interface pages which are displayed.

Both SPs and IDPs MUST ensure this cookie is set to the user's current language preference prior to issuing a message on an HTTP-Redirect or an HTTP-Post binding. Since it is expected that this GC Language Cookie will be used whether or not the user is within an authentication request/response scenario, it should be updated at the earliest possible time.

Details of the GC Language Cookie in the Common Domain are provided in an annex to this document.

### 2.4.4 Name Identifier Management Protocol

A number of GC Departments require notification in the event of a credential revocation. To support this capability, [CATS2 IA&S] adds support for the SAML Name Identifier Management Protocol (and Profile).

SPs specify their desire for receiving these messages by adding a <`ManageNameIDService`> element to their `SPSSODescriptor` in the SP's Metadata.

IDPs MUST send a <`ManageNameIDRequest`> to notify SPs in the event that a NameID previously sent to the SP has been revoked at the IDP. IDPs MUST send these NameID termination messages to SPs for whom they have previously sent assertions for the same principal and SHOULD NOT send these NameID termination messages to other SPs. The messages are sent on the back-channel and SHOULD be sent in a timely manner that is approved by the GCCF. To support this IDPs MUST add a <`ManageNameIDService`> element to their `IDPSSODescriptor` in the IDP's Metadata.

CATS2 makes use of Persistent Anonymous Identifiers (PAIs) which are SAML Persistent Identifiers [SAML2 Core, 3.7] and [SAML2 Errata, E78]. This requires IDPs to maintain "… a persistent opaque identifier for a principal ..." and "A given value, once associated with a principal, MUST NOT be assigned to a different principal at any time in the future."

### 2.4.5 Security

To establish trust and secure communications this interface specification relies heavily on X.509v3 cryptographic key pairs. This section outlines the different certificates that are required as well as specifics on their use.

#### 2.4.5.1 The GC ICM Service Certificates

The GC Internal Credential Management Service (GC ICM), operated by PWGSC on behalf of the GC, provides trust and security to the GC Credential Federation. Possession of valid certificates issued by the GC ICM Service is required for interoperation in the GC Credential Federation. The GC ICM Service issues three certificates to each SP (one used for TLS, one used for digital signature and one used for encryption), and two certificates to each IDP (one used for TLS and one used for digital signature).

- These certificates MUST be maintained in compliance with the Subscriber responsibilities (as specified by the GCCF).

#### 2.4.5.2 Digital Signature

All SAML messages, or parts thereof, MUST be signed by the sender using the GC ICM Service signature certificate that was issued to them. The signature allows the recipient of the message to authenticate the sender, and confirm that the message has not been altered since the time of signature.

- The recipient MUST authenticate the sender and verify the signature upon receipt of the message.
- The recipient MUST verify the revocation status of the sender certificate used to sign the message. Federation member systems MUST use the following method for revocation verification:
    - CRL – the CRL location (in the directory or web site) can be statically configured into the software, and CRL downloaded periodically. See GC ICM documentation (available from GCCF) for details regarding distinguished name location and directory hostname.
- If certificate revocation status cannot be determined, the Federation member system MUST reject the message.

#### 2.4.5.3 Encryption

Encryption ensures that only the intended recipient can decipher the message and gain access to confidential information.

- All confidential information in a SAML message MUST be encrypted.
- Encryption MUST use the public key of the intended recipient’s GC ICM-issued encryption certificate.

#### 2.4.5.4 TLS web sites

##### 2.4.5.4.1 For Front-Channel Bindings

This interface specification specifies front-channel bindings using HTTP over TLS (HTTPS) to transport messages.

- Any site managed by a Federation member and using HTTP bindings over TLS MUST secure the TLS session by using a certificate trusted by default by commercially available browsers.
- Use of SSLv3.0/TLS MUST be compliant with CSE guidelines (e.g., [ITSA-11]) and departmental policies.
- HTTPS over TLS (v1.1 or higher) MUST be used unless not supported by the browser
- HTTPS over TLS (v1.0) MAY be used
- HTTPS over SSL (v3.0 or higher) MAY be used only if TLS (v1.0 or higher) is not supported by the browser .

- Earlier versions of SSL MUST NOT be used

#### 2.4.5.4.2 For Back-Channel Bindings

This interface specification specifies back-channel bindings using SOAP over TLS to transport messages.

- Any site managed by a Federation member and using SOAP Bindings over TLS MUST secure the TLS session by using a certificate trusted by default by commercially available browsers
- Use of SSLv3.0/TLS MUST be compliant with CSE guidelines (e.g., [ITSA-11]) and departmental policies.
- TLS (v1.1 or higher) MUST be used
- Earlier versions of TLS or SSL MUST NOT be used

## 2.4.6 Exception Handling

| Cyber-Auth Interface Support Required | Cyber-Auth Deployment Details |
|---|---|
| The Cyber-Auth member SAML service MUST handle error conditions gracefully | Specifically, the Cyber-Auth member SAML service MUST handle the list of possible errors provided in 2.4.6.1 “Errors to be handled ” |

### 2.4.6.1 Errors to be handled

The following table lists errors that the Federation member SAML service MUST handle gracefully (i.e. in a controlled user-friendly manner as per the ability of the IDP or SP to respond). The table categorizes errors by SAML event.

| Error Condition |
|---|

| |
|---|
| Error Processing <Response><br>• Incorrect/Unknown <Issuer><br>• Incorrect Version<br>• Unrecognized InResponseTo<br>• Unacceptable IssueInstant<br>• Status not Success |
| Error Processing <Assertion><br>• Signature Invalid<br>• Signature Certificate Revoked<br>• Cannot determine revocation status<br>• <Assertion> Time Invalid<br>• Cannot Decrypt <Assertion><br>• Incorrect Recipient<br>• Incorrect Version |
| Error Processing <AuthnRequest><br>• Unknown <Issuer><br>• Signature Invalid<br>• Signature Certificate Revoked<br>• Cannot determine revocation status |
| Error processing SLO Request<br>• Unknown <Issuer><br>• Signature Invalid<br>• Signature Certificate Revoked<br>• Cannot determine revocation status |

Error processing SLO <Response>

- Unknown <Issuer>
- Signature Invalid
- Unknown status
- Signature Certificate Revoked
- Cannot determine revocation status

# Appendix A: Additional Functions Beyond Cyber-Auth (Normative)

## A.1. GC Language Cookie

This Appendix defines a method by which an SP or a IDP can discover which language the principal is currently using. This method relies on a cookie that is written in a domain that is common between IDPs and SPs in the GCCF deployment. This domain is established by the GCCF and may be the same as the Common Domain used for the IDP Discovery Profile and is known as the `<common-domain>` in this profile, and the cookie containing the last language in use is known as the GC Language Cookie.

In the GCCF, both SP and IDP entities are required to host web servers in the common domain as defined by the GCCF.

### A.1.1 GC Language Cookie is in a Common GC Domain

The name of the cookie MUST be "`_gc_lang`". The format of the cookie value MUST be a single valued text string.

The common domain cookie writing service (see below) SHOULD update the language value whenever the user indicates a different language preference. The intent is that the most recently established language is the one in the cookie. The values of the GC language cookie are defined in [ISO 639-2/T]. Acceptable values for the GC Language Cookie include:

- eng
- fra

The cookie MUST be set with a Path prefix of "/". The Domain MUST be set to ".`<common-gc-domain>`" where `<common-gc-domain>` is the common gc domain established by the GCCF for use with this method (it may also be used with the IDP Discovery Profile). There MUST be a leading period. The cookie MUST be marked as secure.

Cookie syntax should be in accordance with IETF RFC 2965. The cookie MUST be session-only.

### A.1.2 Obtaining the GC Language Cookie

Prior to presenting an authentication dialogue to the principal, a IDP MUST know which language the principal desires communication in. To do this, the IDP MUST invoke an exchange designed to present the GC Language Cookie to the IDP after it is read by an HTTP server in the common domain.

The specific means by which the service provider reads the cookie are implementation-specific so long as it is able to cause the user agent to present cookies that have been set with the appropriate parameters. One possible implementation strategy is described as follows and should be considered non-normative. Additionally, it may be sub-optimal for some applications.

- Have previously established a DNS and IP alias for itself in the common domain.
- Redirect the user agent to itself using the DNS alias using a URL specifying "https" as the URL

scheme. The structure of the URL is private to the implementation and may include session information needed to identify the user agent.

- Redirect the user agent back to itself.

### A.1.3 Setting the GC Language Cookie

Prior to invoking an Authentication Request, an SP MUST ensure the GC Language Cookie is set to the principal's preferred language. Prior to sending an Authentication Response (including error responses), an IDP MUST ensure the GC Language Cookie is set to the principal's preferred language. At any time that the principal chooses to change their language, the SP or the IDP MAY set the GC Language cookie. The means by which the SP or IDP sets the cookie are implementation-specific so long as the cookie is successfully set with the parameters given above. One possible implementation strategy follows and should be considered non-normative. The SP or IDP may:

- Have previously established a DNS and IP alias for itself in the common domain.
- Redirect the user agent to itself using the DNS alias using a URL specifying "https" as the URL scheme. The structure of the URL is private to the implementation and may include session information needed to identify the user agent.
- Set the cookie on the redirected user agent using the parameters specified above.
- Redirect the user agent back to itself.

# Appendix B: GCCF Operational Requirements (Normative)

## B.1. Template for GCCF Operational Values

The following GCCF operational values are specified in the document [GCCF Values] which is provided by the GCCF operator.

### B.1.1 Levels of Assurance (LoAs)

The <RequestedAuthnContext> MUST include a Level of Assurance as specified in [SAML2 Assur]. The LoA value will also appear in the <Response> message in the <AuthnContext>.

Also, Metadata for Cyber-Auth IDPs MUST specify the supported Level(s) of Assurance in the <assurance-certification> attribute as defined in [SAML2 Assur], Section 3 Identity Assurance Certification Attribute Profile

The GC Cyber-Auth LoA’s are defined by the GCCF Operator. They must include values for each LoA from LoA1 to LoA4. The values must be unique and stable. There may be multiple values for each LoA (e.g. to satisfy language requirements).

The following table is an example only:

| LoA | Value for <RequestedAuthnContext> |
|---|---|
| 1 | http://cyber-auth.gc.ca/assurance/loa1 |
| 1 | urn:gc-ca: fjgc-gccf:assurance:loa1 |
| 2 | http://cyber-auth.gc.ca/assurance/loa2 |
| 2 | urn:gc-ca: fjgc-gccf:assurance:loa2 |
| 3 | |
| 4 | |

### B.1.2 SPNameQualifier

The GCCF operator may establish affiliation groups of GCCF SPs that will use a common Persistent Anonymous Identifier. In this case SPs MAY use the <SPNameQualifier> in the Authentication Request to indicate their desire for this common PAI. The GCCF operator will also add these affiliation groups to the metadata.

| SPNameQualifier | EntityIDs of GCCF SPs in Group |
|---|---|
| | |
| | |
| | |

### B.1.3 SessionNotOnOrAfter

Cyber-Auth IDP deployments SHOULD NOT specify the SessionNotOnOrAfter attribute. This allows the SP to choose its own required duration for its security context.

If a GCCF IDP is unable to configure this value to not be sent, then it MUST set this value to a high value as determined by the GCCF.

| SessionNotOnOrAfter | GCCF value to be sent |
|---|---|
| | |

### B.1.4 Common Domain Name

There are 2 common domain requirements in this CATS2.document that need to be addressed by the GCCF Operator:

- Section 2.1, eGov 2.5.1 Identity Provider Discovery
    - Cyber-Auth IDP Deployments MUST support the Identity Provider Discovery specified in [SAML2 Prof]
    - Cyber-Auth SP Deployments MAY support the Identity Provider Discovery specified in [SAML2 Prof]
- Appendix A.1 GC Language Cookie
    - “This (GC Language Cookie) domain is established by the GCCF and may be the same as the Common Domain used for the IDP Discovery Profile”

| | Common Domain Value |
|---|---|
| **Identity Provider Discovery** | |
| **GC Language Cookie** | |