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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires
THERE IS A SECURITY REQUIREMENT ASSOCIATED WITH THIS SOLICITATION

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

Issuing Office - Bureau de distribution
Business Transformation and Systems Integration
Service/Division de transformation des opérations et d'intégrat
Special Procurement Initiative Dir
Dir. des initiatives speciales d'approvisionnement
11 Laurier, Place du Portage III
12C1
Gatineau
Québec
KIA 0S5

Title - Sujet ISS Transformation - RFP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 003
Client Reference No. - N° de référence du client 20170549	**Date** 2017-06-02
GETS Reference No. - N° de référence de SEAG PW-$$XE-678-31237	
File No. - N° de dossier 678xe.EP243-170549	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à** 02:00 PM **on - le** 2017-07-14	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** □ **Destination:** ☑ **Other-Autre:** □	
Address Enquiries to: - Adresser toutes questions à: Oates, Christine	**Buyer Id - Id de l'acheteur** 678xe
Telephone No. - N° de téléphone (873) 469-3917 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature**	**Date**

Canada

Amendment Number 003

Purpose:

A. To identify changes to the RFP.
B. To provide answers to questions received with regards to this RFP.

A. CHANGES

Change 21:

At PART 7 – RESULTING CONTRACT CLAUSES, **DELETE** items 7.4.2 through 7.4.7

RENUMBER items 7.4.8, 7.4.9, 7.4.10 and 7.4.11 as 7.4.10, 7.4.11, 7.4.12 and 7.4.13, respectively.

INSERT items 7.4.2 through 7.4.9, as below:

7.4.2. The Contractor/Offeror personnel requiring access to **PROTECTED** information, assets or sensitive work site(s) **must be a permanent resident of Canada or a citizen of Canada and must EACH** hold a valid **RELIABILITY STATUS or SECRET, as required,** granted or approved by CISD/PWGSC.

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

7.4.4. The Contractor personnel requiring access to **NATO RESTRICTED** information or assets) **must be a permanent resident of Canada or a citizen of Canada and must EACH** hold a valid **RELIABILITY STATUS or SECRET, as required**, granted or approved by the appropriate delegated NATO Security Authority.

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

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

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”.*

7.4.8 The contractor should at all times during the performance of the contract possess a letter from PWGSC identifying the results of the FOCI assessment with a FOCI designation of *Not Under FOCI* or *Not Under FOCI through Mitigation*.

7.4.9. All changes to Questionnaire and associated FOCI evaluation factors must immediately be submitted to the Industrial Security Sector (ISS) to determine if the changes impact the FOCI designation.

Change 22:

At PART 7 – RESULTING CONTRACT CLAUSES:

DELETE item 7.28 in its entirety and **REPLACE** with the following:

7.28 Transition Services at End of Contract Period

12 months prior to the expiration of the Contract, the Contractor must prepare and provide the Technical Authority a detailed Service Transition-Out Plan. Upon acceptance of the Technical Authority, the Contractor must transition out its services to another provider in accordance with the Plan, in the period leading up to the end of the Contract Period and for up to three months afterward. The Contractor agrees that there will be no additional charge for these services.

Change 23:

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

DELETE:

APP-IM.16	Enables and supports case file archiving.

INSERT:

APP-IM.16	Enables and supports case file archiving from within the Solution.

Change 24:

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

DELETE:

APP-IM.27	Enables Internal Users to retrieve archived records from a case file for a specified retention time, determined by the business process.

INSERT:

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.

Change 25:

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

DELETE:

APP-COM.03	Enables External Users to automatically receive standardized text notifications resulting from predefined events such as decision made regarding the service request.

INSERT:

APP-COM.03	Enables External Users to automatically receive standardized email notifications resulting from predefined events such as decisions made regarding the service request.

Change 26:

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

DELETE:

AP-PPL.02	Enables the scanning of paper documents for appendage to case files.

INSERT:

AP-PPL.02	Enables the attachment of scanned documents to case files.

Change 27:

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

DELETE:

WP-UE.09	Enables External Users to receive SMS standardized messages pertaining to service request updates.

INSERT:

WP-UE.09	Enables External Users to receive standardized email messages pertaining to service request updates.

Change 28:

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

DELETE:

WP-RP.01	Usage Reporting: Provides the ability to collect and report on usage information according to GC standards.

Change 29:

At ANNEX A, Section 3, under 1.1 Requirement Overview:

DELETE:

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

INSERT:

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

Change 30:

DELETE:

Figure 2: High level ISST Solution architecture diagram

Change 31:

At Section 3, 1.1 Requirement Overview, paragraph 3:

DELETE:

External Users, such as Contract Security and Controlled Goods Program applicants, will access the functionality required for their business processes via the internet Web Portal, based on the Adxstudio technology.

INSERT:

External Users, such as Contract Security and Controlled Goods Program applicants, will access the functionality required for their business processes via the internet Web Portal.

Change 32:

At Section 3, 1.1 Requirement Overview:

DELETE:

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

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

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

(b) **Dynamics CRM (On premise) 2015 (or higher)**
Case Management Technology - The portal will interface with a Customer Relationship Management tool, MS Dynamics CRM (on premise) 2015 (or higher), to initiate, interact with,

manage and perform case management activities. The Case Management tool is a centrally managed service and will be used by Internal Users having defined roles and rights.

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

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

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

INSERT:

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

(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.

Controlled access for External Users will be through an internet-based user-centric web portal interface. The web portal must be developed as a CRM customer portal based on a COTS portal technology (on premise), and must host web enabled forms for the requisition of and receipt of services. 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 configured web portal must meet GC requirements (WCAG) for web standards.

Change 33:

At Section 3, 1.1 Requirement Overview:

INSERT:

(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.

Change 34:

At ANNEX A, Section 3, 1.2 Detailed Requirements:

DELETE Tech.12 in its entirety and **REPLACE** with:

Tech.12	Utilizes a COTS web portal technology to create a web portal, with 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.

Change 35:

At ANNEX A, Section 3, 1.2 Detailed Requirements:

DELETE Tech.17 in its entirety and **REPLACE** with:

Tech.17	Meets at a minimum “Protected B, High Integrity, Medium Availability” (PB/H/M) security profile requirement.

Change 36:

At ANNEX A, Section 3, 1.2 Detailed Requirements:

DELETE Tech.18 in its entirety and **REPLACE** with:

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 COTS Web Portal.

Change 37:

At ANNEX A, Section 4, under 1.2.1 Internal Users:

DELETE:

SecureInt.05	Ensures that SCMS is accessible through a VPN.

INSERT:

SecureInt.06	Ensures that Microsoft Dynamics CRM is accessible through a VPN.

Change 38:

At ANNEX A, Section 5, 1.1.2 Security Control Catalogue:

DELETE:

The following provides a very high level description of the Information Technology Security Guidance 33 (ITSG-33) security control catalogue which is organized into classes and control families. These control families apply to the ISS security requirements and are further addressed by the Detailed Requirements defined in this ANNEX. The controls satisfying the full Solution are embedded in the existing technical implementations, such as the SCMS. Since the full Solution will be primarily an integration exercise, the full suite of Solution controls will be assessed throughout the development of the Solution using the Security Assessment and Authorization process. These control families are the basis of securing the Solution and its Data.

INSERT:

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.

Change 39:

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

DELETE:

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

INSERT:

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.

Change 40:

At ANNEX A, Section 5, 1.2 Detailed Requirements:

DELETE SC.15 in its entirety and **REPLACE** with:

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.

Change 41:

At ANNEX A, Section 5, 1.2 Detailed Requirements:

DELETE SC.28 in its entirety and **REPLACE** with:

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.

Change 42:

At ANNEX A, Section 5, 1.2 Detailed Requirements:

DELETE SC.41 in its entirety and **REPLACE** with:

SC.41	The Solution, at a minimum, must comply with the requirements for PB/H/M.

Change 43:

At ANNEX A, Section 7, under 1.3 Detailed Requirements – Project Management, item PM.04:

INSERT:

(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.

(f) Except where otherwise specified, all project work that does not require direct access to ISS information and assets can be done off-site.

Change 44:

DELETE ANNEX C – SRCL in its entirety, and **REPLACE** with the attached ANNEX C – SRCL.

Change 45:

At ANNEX F – Resource Category Information for Optional Services, under 3.9.2 Minimum Mandatory Qualifications:

DELETE M4 in its entirety and **REPLACE** with the following:

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.

B. Questions

Question 10:

Would the Crown please confirm that all work related to the project must/will be completed in government offices?

Answer 10:

The Crown confirms that not all work related to the project must be completed within a government facility. It is expected that the Senior Delivery/Project Manager and Project Management Team (See ANNEX A, Section 7) be located on-site and to be available to the Project Authority as required in order to attend meetings, provide updates, address concerns, etc.

As noted in the SRCL, Part C, the Contractor will not receive or store, nor use their own IT systems to process or store PROTECTED and/or CLASSIFIED information or assets. The Contractor will also not be provided with an electronic link between the Contractor's IT systems and the government department, in this case PWGSC.

As such, all project work that requires an individual to have direct access to ISS information and assets will be required to be on-site for the duration of that work. Once that work has been completed, those resources are no longer required to be on-site. Any project work that does not require direct access to ISS information and assets can be done off-site. To assist in clarifying work location, additional requirements have been added to ANNEX A, Section 7, PM.04. Please see Change 43 in this Amendment.

Question 11:

Would the Crown please clarify if any personal information from the European Union that could fall under the General Data Protection Regulation (GDPR) is contained within or handled by the Solution?

Answer 11:

The Solution will not contain or handle any information that is subject to the GDPR.

Question 12:

The RFP outlines that 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 in Appendix 4 to Annex A. The Contractor may not be aware of legislative changes or amendments to policies without being advised by Canada during the fulfillment of the contract. Therefore, we respectfully suggest that the Crown should add a statement that "Canada will advise the Contractor of any additional policies, directives, and guidelines, as required."

Answer 12:

Please see Change 20 in Amendment 002, wherein the following statement was added to Appendix 4 to Annex A : "The Project Authority will advise the Contractor of any new or amended federal legislation, regulations, policies, directives, standards and guidelines that impact the project".

Question 13:

The Section 1.2.1 Internal User requirements list has a duplicated SOW Number SecureInt.05. Can the second requirement be renumbered to be next in sequence? It would be: SecureInt.06 Ensures that SCMS is accessible through a VPN.

Answer 13:

SecureInt.05 is identified twice in error. Please see Change 37 in this Amendment.

Question 14:

Can it be assumed that the solution will have access to peer test systems (government and third party) for integration testing of the solution?

Answer 14:

The Contractor will need to detail all requirements for testing within their testing plan. Environments will be provided based upon approval of those plans. The PWGSC project team will organize and coordinate the solution integration testing internally, with the security partners (e.g. RCMP, CSIS) and third party organizations (e.g. Credit Bureau). The Contractor will be responsible for the detailed aspects of the integration testing with the security partner and third party representatives.

Question 15:

Mandatory Requirement M1/M2 specify that the "Bidder must provide three (3) Reference Projects similar to that of ANNEX A, Sections 2 through 7, completed within fifteen (15) years of the date of Bid Closing and have a public-facing internet-based information exchange component."

In our experience, we have similar Federal Government intranet-facing projects which meet or exceed the volumes requested in M1 and M2 as well as align closely to the remaining M1 and M2 requirements. Given that the core requirements of the reference projects relate to BPR/CM/CRM, we believe that showing a web based component which is either internet-based OR an intranet-based should be sufficient to meet PSPC's requirements.

We therefore ask that the M1 and M2 requirements be modified to include "a public facing internet or intranet-based information exchange component".

Answer 15:

Mandatory Criteria M1 and M2 in the Technical Evaluation currently states, "The Bidder must provide three (3) Reference Projects similar to that of ANNEX A, Sections 2 through 7, completed within fifteen (15) years of the date of Bid Closing and have a public-facing internet-based information exchange component". The public-facing internet exchange component is pertinent as the final solution will be utilized in the same fashion. As a result, a Federal Government intranet-based information exchange project would be deemed non-compliant as the security requirements would be different than those for a public facing internet project.

Question 16:

Will the Contractor be able to reuse the existing information exchange channel implementations for communicating with PSPC ISS security partners, including RCMP, CSIS, CSE, DND, Credit Bureau/Equifax? If yes, can the contractor assume that these implementations meet the data in-motion and at-rest requirements for the ISST program?

Answer 16:

The Contractor should not assume that any existing information exchange channel; complies with the proposed architecture, complies with security requirements, or meets business process requirements.

Question 17:

SC.33 - The Contractor must report all suspected or actual privacy and security violations as Security Incidents for the duration of the contract. Can GC confirm or elaborate on the scope of this item. Are these just violations internally within the contractor OR is there an expectation that the contractor is performing some form of comprehensive monitoring of the environments?

Answer 17:

The intent of this requirement is purely reporting of actual privacy and security violations throughout the Contract. For example, if the Contractor suspects or witnesses or has evidence that any individual, Contractor or other, is tampering with the data or the system configuration, this incident must be reported to GC.

Question 18:

In reference to Call Centre Integration:

Can PSPC confirm that there is no integration between call center technology and the Solution?

Answer 18:

At this time there is no plan to integrate existing call center technology and the Solution.

Question 19:

In reference to Annex A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-IM.16 (page 20 or 70);

Is this only archiving within the solution and/or the solution's ability to interact with a 3rd party archiving solution? If a 3rd party solution, please provide the additional requirements such as interface specification, frequency, etc.

Answer 19:

With respect to ANNEX A, Section 2, business requirement APP-IM.16, case file archiving is expected to be completed within the Solution. Please see Change 23 in this Amendment.

Question 20:

In reference to Annex A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-IM-27 (page 21 0f 70);

Is this only archiving within the solution and/or the solution's ability to interact with a 3rd party archiving solution? If a 3rd party solution, please provide the additional requirements such as interface specification, frequency, etc.

Answer 20:

With respect to ANNEX A, Section 2, business requirement APP-IM.27, case file archiving and the access to archived case files is expected to be completed within the Solution. An amendment has been made to APP-IM.27 for clarification. Please see Change 24 in this Amendment.

Question 21:

In reference to Annex A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-COM.03 (page 21 of 70) and 2.2.2 Web Portal, WP-UE.09 (page 27 of 70);

Will GoC be providing the SMS gateway? If so, please provide the interface specifications and any constraints related to its usage.

Answer 21:

With respect to ANNEX A, Section 2, business requirements APP-COM.03 and WP-UE.09, currently PWGSC currently does not have a SMS gateway. Requirements APP-COM.03 and WP-UE.09 have been amended to replace SMS with standardized email messages. Please see Changes 25 and 27 in this Amendment.

Question 22:

Do you currently have a text messaging provider? If yes, please indicate which provider.

Answer 22:

Please see response to Question 21 in this Amendment.

Question 23:

In reference to Annex A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-COM.06 (page 21 0f 70) ;
(a) **Question:** How are the postal mailings to be accomplished? Is the solution solely required to print, then handled by staff, or is there an interface file that is required to be created and sent to a 3rd party?
(b) **Question:** Are there specific volumetrics and time to complete measures that should be considered?

Answer 23:

With respect to ANNEX A, Section 2, business requirement APP-COM.06, printed correspondence will be manually mailed by PWGSC. At this time there are no volumetric or time to complete measures to be considered.

Question 24:

In reference to ANNEX A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-PPL.02 (page 21 0f 70);
Is this simply the ability to attach an image to a case file?

Answer 24:

With respect to ANNEX A, Section 2, business requirement APP-PPL.02, this is the ability to scan a document using an external to the Solution scanner and to be able to attach that scanned file to a case file within the Solution. The Solution is not expected to interface with external scanners. An amendment has been made to ANNEX A, requirement AP-PPL.02 for clarification. Please see Change 26 in this Amendment.

Question 25:

In reference to Annex A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-RP.03 (page 23 of 70);
Do you have specific measurement criteria that you are looking to have monitored related to individual workloads?

Answer 25:

With respect to ANNEX A, Section 2, business requirement APP-RP.03, at this time there is no specific measurement criteria for monitoring individual workloads.

Question 26:

In reference to Annex A, Section 2: Business Requirements, 2.2 Detailed Requirements – Functional Requirements, 2.2.2 Web Portal, WP-RP.01 (page 28 of 70);
What is considered the “GC Standards”?

Answer 26:

With respect to ANNEX A, Section 2, business requirement WP-RP.01 has been removed as the other reporting requirements within the Web Portal component of the Solution will satisfy the ISS business needs. Please see Change 28 in this Amendment.

Question 27:

In reference to Section 7.15.2 (page 35 of 40) and Section 7.15.3 (page 35 of 40) of the RFP, does PWGSC agree to amend the RFP such that the limit of liability contained in Section 7.15.2(e)(ii) applies also to any and all claims, whether first party or third party, and all resulting damages related to infringement of intellectual property rights?

Answer 27:

PWGSC does not agree to amend the limitation of liability clauses present at item 7.15. These clauses are standard TB approved clauses that have been developed in consultation with industry specifically for the IM/IT commodity grouping.

Question 28:

In reference to Section 7.15.2 of the RFP (page 35 of 40), does PWGSC agree to amend the RFP such that the limit of liability contained in Section 7.15.2(e)(ii) applies also to breaches by the Contractor of its confidentiality provisions but only in relation to personal information as defined by applicable privacy law?

Answer 28:

See response to Question 27 in this Amendment.

Question 29:

In reference to Section 7.15.2(e)(ii) of the RFP (page 35 of 40), does PWGSC agree to substitute the 0.75 by 0.25?

Answer 29:

See response to Question 27 in this Amendment.

Question 30:

In section 7.2.1.9, under Canada's Obligation, the RFP states that Canada reserves the right to acquire the work by other means. The RFP contemplates a significant business process re-design and a system implementation. Since the RFP is being sourced through a competitive process where Canada will have opportunity to evaluate the Bidder's proposed plans and approaches, we do not understand why Canada would include such a requirement in addition to the termination clauses and penalties provided in the Resulting Contract Clauses. We respectfully request that the reference be removed, as it could be used to undermine the relationship between the Bidder and Canada, as an alternative to the dispute resolution and termination provisions.

Answer 30:

The clause at item 7.2.1.9 refers to the portion of the Work to be performed under the Contract on an "as and when requested basis" using a Task Authorization, as described under 7.2 Task Authorization and sub-articles. It is not intended to undermine the relationship between the Bidder and Canada. Canada does not agree to amend the clause at the present time.

Question 31:

With respect to item 7.28: within the draft RFP, there was a 3-month limit for transition services at no charge at the end of the contract. In the final version of the RFP, the Bidder must commence transition services 12 months prior to the expiration date of the contract, and for an unknown period. This change puts the Bidder at significant risk since termination provisions favour the Crown and there is no cap on the requirement. In our experience, these types of criteria will cause bidders to add contingency and cost to their bids as a protection against the risk, artificially increasing the cost to Canada. We respectfully request that the 3-month cap be re-instituted in the RFP, for clarity and to protect the Bidder against unknowns that will artificially inflate costs.

Answer 31:

Canada has amended item 7.28 to limit the period of transition services. Please see Change 22 in this Amendment.

Question 32:

Both the body of the RFP, as well as the accompanying SRCL, indicate that the bidder may use resources from outside of Canada (i.e. NATO). Given that the system will be collecting, storing, and processing sensitive personal background data on Canadian citizens for security clearances up to and including Government of Canada Top Secret, can PSPC please confirm that it is not their intent to restrict the bidders as follows:

a. Bidders qualified as Canadian company's under FOCI; and
b. Bidder resources (especially those with access to technical, design and operational details) to Canadian citizens, or other appropriate national security exclusions?

Answer 32:

The SRCL has been amended, with changes to Part A, items 7b) and 9, to indicate that this procurement is restricted to Canada, including permanent residents, and that the supplier will be required to access INFOSEC information or assets. Part 7, item 7.4 of the RFP has also been amended with the new security requirements related to the above changes, including a requirement for a Foreign Ownership, Control and Influence assessment. Please see changes 21 and 44 in this Amendment.

Question 33:

Certain areas of Figure 2 of ANNEX A – Statement of Work are highlighted indicating "Procurement Ongoing".

a. Does the term "Procurement Ongoing" refer to the current PSPC ISST Solicitation or to other procurements?
b. Is the implementation of these areas within the scope of the PSPC ISST Solicitation?
c. If these areas are NOT within the scope of the PSPC ISST Solicitation what are the specific products or services that will be used to implement the following areas in the diagram?
    I. Imaging/Scanning System
    II. Documents and Records Management System
    III. Forms Management

Answer 33:

Figure 2 is currently under review, please see response to Question 35 in this amendment.

However, the following is still applicable for the Solution.

a. The term "Procurement Ongoing" will be replaced by the term 'Under development'.

b. The Contractor is not responsible for the implementation of these areas. The Contractor is responsible for all software configurations, development and integrations required for the ISST Solution in accordance with the Statement of Work leveraging the proposed technology platforms as outlined in ANNEX A. For example GCIP platform and its capabilities will be available for the Contractor to configure when developing necessary messaging specifications required for exchanging information with partner organizations.

c. The Contractor must leverage the proposed technology platforms as outlined in Annex A to configure, develop and integrate the technologies to form the ISST Solution in accordance with the Statement of Work. These areas are all within the scope of the ISST Solution configuration mainly from an integration perspective.

    i. Imaging/Scanning System: This system is in place and uses IBM DataCap technology. The ISST Solution will need to receive information with this system.

    ii. 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.

    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.

    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.

iii. Forms Management: Electronic fillable forms are created using Adobe products, however, the Contractor is not responsible for form creation. There are two scenarios regarding the electronic fillable forms:

1. Users can complete their request using the web portal, but instead of submitting electronically, they choose to either save as a file or print it off. The resulting output should be a read only pdf with a barcode that can be scanned upon receipt at ISS for input and processing.
2. As a part of the ISS business continuity plan, if the system is down, users would have the ability to download a fillable pdf, fill it out locally and submit to ISS. This pdf would create a barcode, similar to scenario 1, which would be scanned upon receipt at ISS for input.

Canada is not looking for the Solution to create these fillable electronic pdf forms.

Please see Change 33 in this Amendment.

Question 34:

One of the mandatory requirements refers to a TBS policy for desktop productivity citing the Microsoft suite as a basis for the requirement, and appearing to include the ADX Studio in this suite. However, ADX Studio was not part of the original Desk Top suite as Microsoft had not acquired the company as of the award date.

What is the basis for the inclusion of ADXstudio and will the Crown amend the SOW to allow other web portal technologies to be considered?

Answer 34:

The basis for the inclusion of ADXStudio was that it meets the platform compatibility and case management integration requirements for the Solution. Canada will consider the use of other proposed commercial off the shelf (COTS) web portal technologies, provided that they meet the Solution requirements. The SOW will be amended to reflect the removal of ADXStudio as the COTS web portal technology. Please see Changes 31, 32, 34, 36 and 45 in this Amendment. Additional requirements for a COTS web portal will be provided in a forthcoming amendment.

Question 35:

Issue – Security Scope: The RFP has stated an extensive, all-inclusive set of Government security & privacy standards and policies as references within the RFP. Also contained in that document are a number of security requirements, which includes a broad non-specific requirement to be compliant with the CSE ITSG-33 Protected B Medium Medium profile. That profile contains 428 controls and sub-controls, many of which are beyond the currently defined scope of the RFP.

Risk/Impact: The greatest risk for a bidder is to bid on services where the scope is not well defined and where the potential cost variances are substantial. Unless more clarity can be brought to the exact security (and security control) requirements, there is a significant potential risk to both the bidder and PSPC for cost, effort and schedule.

Recommendation: It is strongly recommended that PSPC more clearly define exactly what security requirements a bidder will have to achieve for a successful delivery. This includes specifying which controls in the ITSG-33 profile are applicable (such as selected controls in the IT Projects column), which are the responsibility of the bidder, and which are the responsibility of Canada as the host and operator of the supplied capability.

Answer 35:

As a result of an ongoing review of the business needs for security, it has been determined that the appropriate security profile for the Solution is Protected B, High Integrity, Medium Availability (PB/H/M). This represents a change from the current security profile identified in the SOW. Therefore, additional security controls must be applied to the solution. These additional security controls are provided for reference as an attachment to this amendment. However, the new security requirements resulting from the security profile change and the new controls will be provided in a forthcoming amendment to Section 5. Note that not all ITSG-33 controls are to be implemented by the Contractor. Many of the technologies to be integrated are implemented and have security controls in place. As well, security controls / requirements pertinent to the infrastructure will be implemented by Shared Services Canada. The SOW only contains those requirements which require effort on the part of the Contractor. It should also be noted that during the Contract period, as the architecture is further developed, additional security controls may arise or be recommended through the SA&A process (see Section 5: IT Security Requirements, 1.1.1 Security Assessment and Authorization Process). Please refer to Changes 29, 30, 35, 39, 40, 41 and 42 in this Amendment for changes related to the solution's security profile. Additionally, refer to the Additional Security Controls document, provided as an attachment to this Amendment.

Question 36:

Annex A - Statement of Work, SECTION 5: IT SECURITY REQUIREMENTS, 1.2 DETAILED REQUIREMENTS, SC.41 (page 47 of 70) calls into play the entire Protected B Medium control set from ITSG-33. This includes many controls that appear to be well beyond the scope of the RFP (e.g. network, SOC, monitoring and SIEM services).

Could PSPC please indicate which of those controls are the responsibility of the bidder, and which would be satisfied by Canada?

Answer 36:

Please see response to Question 35 in this amendment.

Question 37:

The conceptual architecture in Section 3, 1.1 identifies the SCMS iteration of MS Dynamics CRM as the required case management solution. The paragraph following the conceptual architecture does not specify SCMS but does identify MS-Dynamics CRM 2015 as the intended Case Management technology for the solution. Would the Crown be able to clarify whether Microsoft Dynamics CRM 2015, or the SCMS implementation of MS-Dynamics, is the intended CRM solution platform.

Answer 37:

PWGSC has standardized on the use of Microsoft Dynamics CRM 2015 (or higher) as the development platform for Case Management applications. This is the required platform for the ISST Solution. The SCMS instance of Microsoft Dynamics CRM, including associated functionalities and standards, should be leveraged where possible and will be made available to the Contractor in order to identify areas of applicability. An amendment has been made to replace references to SCMS with Microsoft Dynamics CRM. See Changes 37 and 38 in this Amendment.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

Government of Canada Gouvernement du Canada

Contract Number / Numéro du contrat

EP243-17-0549 (Rev #3)

Security Classification / Classification de sécurité

Unclassified

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization
Ministère ou organisme gouvernemental d'origine

Public Services and Procurement Canada

2. Branch or Directorate / Direction générale ou Direction

Departmental Oversight Branch

3. a) Subcontract Number / Numéro du contrat de sous-traitance

3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work - Brève description du travail

Industrial Security Systems Transformation Project
The objective of this procurement is to acquire System Integration Services in support of project delivery

5. a) Will the supplier require access to Controlled Goods?
Le fournisseur aura-t-il accès à des marchandises contrôlées? ☑ No Non □ Yes Oui

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?
Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? ☑ No Non □ Yes Oui

6. Indicate the type of access required - Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?
Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?
(Specify the level of access using the chart in Question 7. c)
(Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) □ No Non ☑ Yes Oui

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas?
No access to PROTECTED and/or CLASSIFIED information or assets is permitted.
Le fournisseur et ses employés (p.ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes?
L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. ☑ No Non □ Yes Oui

6. c) Is this a commercial courier or delivery requirement with no overnight storage?
S'agit-il d'un contrat de messagerie ou de livraison commerciales sans entreposage de nuit? ☑ No Non □ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☑	Foreign / Étranger □

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions Aucune restriction relative à la diffusion □	All NATO countries Tous les pays de l'OTAN □	No release restrictions Aucune restriction relative à la diffusion □
Not releasable À ne pas diffuser □		
Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☑	Restricted to: / Limité à : □
Specify country(ies): / Préciser le(s) pays : Restricted to Canada, including permanent residents	Specify country(ies): / Préciser le(s) pays : Restricted to Canada, including permanent residents	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A PROTÉGÉ A ☑	NATO UNCLASSIFIED NATO NON CLASSIFIÉ ☑	PROTECTED A PROTÉGÉ A □
PROTECTED B PROTÉGÉ B ☑	NATO RESTRICTED NATO DIFFUSION RESTREINTE ☑	PROTECTED B PROTÉGÉ B □
PROTECTED C PROTÉGÉ C □	NATO CONFIDENTIAL NATO CONFIDENTIEL □	PROTECTED C PROTÉGÉ C □
CONFIDENTIAL CONFIDENTIEL □	NATO SECRET NATO SECRET □	CONFIDENTIAL CONFIDENTIEL □
SECRET SECRET □	COSMIC TOP SECRET COSMIC TRÈS SECRET □	SECRET SECRET □
TOP SECRET TRÈS SECRET □		TOP SECRET TRÈS SECRET □
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) □		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) □

Security Classification / Classification de sécurité

Unclassified

Canada

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité : ☑ No Non □ Yes Oui

9. Will the supplier require access to extremely sensitive INFOSEC information or assets:
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? □ No Non ☑ Yes Oui

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS COTE DE FIABILITÉ	□ CONFIDENTIAL CONFIDENTIEL	☑ SECRET SECRET	□ TOP SECRET TRÈS SECRET
□ TOP SECRET - SIGINT TRÈS SECRET - SIGINT	□ NATO CONFIDENTIAL NATO CONFIDENTIEL	□ NATO SECRET NATO SECRET	□ COSMIC TOP SECRET COSMIC TRÈS SECRET
□ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : See attached Security Specification Guide

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? ☑ No Non □ Yes Oui

If Yes, will unscreened personnel be escorted:
Dans l'affirmative, le personnel en question sera-t-il escorté? ☑ No Non □ Yes Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? ☑ No Non □ Yes Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? ☑ No Non □ Yes Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matérial PROTÉGÉ et/ou CLASSIFIÉ? ☑ No Non □ Yes Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? ☑ No Non □ Yes Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? ☑ No Non □ Yes Oui

PART C *(continued)* / PARTIE C *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Intenet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	Confidential Confidentiel	Secret	Top Secret Très Secret	NATO Restricted NATO Diffusion Restreinte	NATO Confidential NATO Confidentiel	NATO Secret	COSMIC Top Secret COSMIC Très Secret	Protected Protégé			Confidential Confidentiel	Secret	Top Secret Très Secret
											A	B	C			
Information / Assets Renseignements / Biens																
Production																
IT Media Support TI																
IT Link Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No Non □ Yes Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée.

12. b) Will the document attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No Non □ Yes Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Note: Controls description based on 30 December 2014 version of ITSG-33 Annex 3A Security Control Catalogue

Suggested Assignment
R=Responsible, S=Support

Family	**Control ID**	**Enhancement**	**Name**	**Class**	**Definition**	**Supplemental Guidance**	IT Security Function	IT Operations Group	IT Projects	Physical Security Group	Personnel Security Group	Learning Center	**General Tailoring and Implementation Guidance Notes**
AC	2	(11)	ACCOUNT MANAGEMENT	Technical	ACCOUNT MANAGEMENT | USAGE CONDITIONS The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].	Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.		S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.

AC	10		CONCURRENT SESSION CONTROL	Technical	(A) The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts	S		R				
AU	3	(2)	CONTENT OF AUDIT RECORDS	Technical	CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].	This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.	S	R	S				This security control/enhancement cannot be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, implementation of this security control/enhancement may be somewhat problematic.

AU	5	(2)	RESPONSE TO AUDIT PROCESSING FAILURES	Technical	RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).	S		R				

AU	10		NON-REPUDIATION	Technical	(A) The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].	Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.

AU	12	(3)	AUDIT GENERATION	Technical	AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].	This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7			R				
CM	2	(3)	BASELINE CONFIGURATION	Operational	BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.	Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.		R					

CM	3	(1)	CONFIGURATION CHANGE CONTROL	Operational	CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or have been disapproved by [Assignment: organization-defined time period]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.		S	R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.

CM	7	(2)	LEAST FUNCTIONALITY	Operational	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Related control: CM-8.			R				
IA	2	(1)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	Technical	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to privileged accounts.	Related control: AC-6.			R				ISS Details: Add safeguard, external LOA2, internal LOA3.
IA	2	(2)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	Technical	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to non-privileged accounts.				R				ISS Details: Add safeguard, external LOA2, internal LOA3.

IA	2	(3)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	Technical	IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to privileged accounts.	Related control: AC-6.			R				This security control/enhancement is considered a compensating control that should be applied if the capability cannot be addressed using an alternate security control/enhancement. All management should be done in a controlled zone. This security control/enhancement could be used to strengthen the audit capability if a TRA has identified an insider threat.
IA	2	(4)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	Technical	IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to non-privileged accounts.				R				

IA	5	(11)	AUTHENTICATOR MANAGEMENT	Technical	AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].	Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.
IR	4	(1)	INCIDENT HANDLING	Operational	INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process.	Automated mechanisms supporting incident handling processes include, for example, online incident management systems.	S	R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.

SA	4	(2)	ACQUISITION PROCESS	Management	ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].	Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.	S		R				

SA	4	(9)	ACQUISITION PROCESS	Management	ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.			R				

SC	4		INFORMATION IN SHARED RESOURCES	Technical	(A) The information system prevents unauthorized and unintended information transfer via shared system resources.	This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. However, this security control/enhancement cannot be met using readily available COTS components. Consequently, implementation of this security control/enhancement may be problematic.

SI	6		SECURITY FUNCTIONAL VERIFICATION	Operational	(A) The information system verifies the correct operation of [Assignment: organization-defined security functions]. (B) The information system performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]. (C) The information system notifies [Assignment: organization-defined personnel or roles] of failed security verification tests. (D) The information system [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	Transitional states for information systems include, for example, system start-up, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6	S	R	S				

SI	7	(5)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	Operational	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.	Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.	S	R	S				