



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 spéciales

d'approvisionnement

11 Laurier, Place du Portage III

12C1

Gatineau

Québec

K1A 0S5

Title - Sujet ISS Transformation - RFP	
Solicitation No. - N° de l'invitation EP243-170549/B	Amendment No. - N° modif. 007
Client Reference No. - N° de référence du client 20170549	Date 2017-07-25
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 2017-08-11	Time Zone Fuseau horaire Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input checked="" type="checkbox"/> Other-Autre: <input type="checkbox"/>	
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

Amendment Number 007

Purpose:

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

A. CHANGES

Change 61:

At ANNEX A, Section 2 Business Requirements, under 2.2 Detailed Requirements, **DELETE** APP-ICN.01 in its entirety and **REPLACE** with the following:

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.

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.

Change 62:

At ANNEX A, Section 2: Business Requirements, under 2.2 Detailed Requirements, **DELETE** APP-ICN.10 in its entirety.

Change 63:

At ANNEX A: Section 5: IT Security Requirement, under 1.2 Detailed Requirements, **DELETE** SC.18 in its entirety and **REPLACE** with the following:

The Contractor must provide a Security Detailed Solution 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.

Change 64:

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

INSERT:

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.
---------------------------------------	-------	--

Change 65:

At APPENDIX 5 to ANNEX A – Glossary:

INSERT:

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

Note: The following changes 66 to 71 apply to Attachment 1 to Part 4: Technical Evaluation

Change 66:

At 3. Mandatory Criteria, **DELETE** M1, Item D, Sub-item iv. in its entirety and **REPLACE** with the following:

Budget management (including the overall cost of services contracted for, both at contract award and at contract closeout);

Change 67:

At 4. Point Rated Criteria, R1, Item A:

DELETE:

Project Governance and Team Structure Document, including the following:

INSERT:

Project Governance and Team Structure, including the following:

Change 68:

At 4. Point Rated Criteria, R1, Item B:

DELETE:

Scope Management Plan describing how scope will be managed throughout the Project Delivery Stage. This narrative should address the following:

INSERT:

Scope Management describing how scope will be managed throughout the Project Delivery Stage. This narrative should address the following:

Change 69:

At 4. Point Rated Criteria, R1, Item C:

DELETE:

Schedule Management Plan that outlines the Bidder's strategy for managing ISST project activities. The response should contain the following:

INSERT:

Schedule Management that outlines the Bidder's strategy for managing ISST project activities. The response should contain the following:

Change 70:

At 4. Point Rated Criteria, R1, Item E:

DELETE:

Risk Management Plan, in alignment with NPMS that includes the following:

INSERT:

Risk Management, in alignment with NPMS that includes the following:

Change 71:

At 4. Point Rated Criteria, R1, Item F:

DELETE:

Quality Management Plan that outlines the Bidder's strategy to ensure that quality is integrated into project management and product development, deliverables and processes, from both a business process and solution implementation perspective. The response should contain the following:

INSERT:

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:

B. QUESTIONS

Question 84:

In section 7.26, there is a requirement for Daily and weekly time reporting. Given that this is a fixed price solution, the need for time and task reporting is not necessary. Would the Crown please remove this criterion?

Answer 84:

Canada does not anticipate a requirement for exhaustive time and task reporting. However, Canada may require the information described under Part 7 – Resulting Contract Clauses, article 7.26, for project planning activities or for other purposes. Therefore, Canada will not amend the clause at 7.26.

Question 85:

Would the Crown replace: 4007 (2010-08-16), Supplemental General Conditions - Canada to Own Intellectual Property Rights in Foreground Information; with 4006 (2010-08-16), Contractor to Own Intellectual Property Rights in Foreground Information and have it apply to and form part of the Contract?

Answer 85:

Canada has a requirement to maintain Intellectual Property Rights in Foreground Information, and will not replace or amend 4007 (2010-08-16), Supplemental General Conditions – Canada to Own Intellectual Property Rights in Foreground Information.

Question 86:

Would it be possible to obtain more detailed information on the Data Sources for the migration effort estimation? We would like to see all of the sample data sets that will be provided so that we can begin to derive the architecture of the data being delivered (DB's per source system, table count per database, detailed table structure information, column names per table, formats per column, min/max values, etc.).

Answer 86:

At this time all data sources have not been identified. Sample data will be provided to the Contractor upon contract award for detailed database design. Please refer to Question 69 in Amendment 006 for some information regarding the databases.

Question 87:

Please clarify the Scope of the migration effort:

- a) Is it only a migration from the identified Source systems to the Dynamics CRM environment?
- b) Are we expected to provide migration scripts from web-based systems as in scope?
- c) Are we expected to provide migration scripts to cover movement to the BI sub-system?
- d) If the actual data is in a Sybase/Access/other format, will the sample data also be in this format thus requiring transformation of sample data as part of the migration efforts?

Answer 87:

With respect to the scope of the data migration effort:

- a) The data migration effort includes the migration of data from current ISS legacy system databases and any identified external data sources (e.g. excel files, access databases, etc.) into the Solution environment.
- b) Migration scripts are expected to include the movement of data from the current web-based internet and intranet solutions used by the ISS. These are included in our portfolio of legacy data for migration.
- c) If the Contractor identifies that CRM does not provide all required functionality to satisfy the Solution's reporting requirements, then a script will be required to populate the BI sub-system. If the Solution's reporting requirements can be satisfied with only CRM functionality, no script is required. Please see the response to Question 140 in this Amendment for more information.
- d) At this time the sample data has not been created. The data will be provided in the required formats to ensure scripting accuracy.

Question 88:

How many years of data (current and historical) will be stored within the system?

Answer 88:

Data belonging to active records must be stored within the Solution for reference, review, reporting and other business needs. Currently, the oldest active file within the existing system is 20 years old. However, the new Solution must permit indefinite storage for active records.

Question 89:

In reference to Annex A – Statement of Work, 2.2 Detailed Requirements – Functional Requirements, 2.2.1 Service Processing Application, APP-COM.05 (page 21 of 70); Microsoft Dynamics CRM uses Exchange to send emails. We do not recommend this procedure for clients that want to do mass email. Mass emailing usually requires an external third party.

- a) How many email messages could be sent simultaneously to External Users (5-10, 50 or more, 1000 and more)?
- b) Are you also looking to send text messages to targeted groups of external users?

Answer 89:

With respect to requirement APP-COM.05:

- a) The purpose of this requirement is the ability to send to targeted groups and not in mass emails. We send one email message to approximately 5000 users in batches of 500 recipients at a time.
- b) There is no requirement to send SMS messages at this time as per amendments to APP-COM.03 and WP-UE.09. Please refer to Change 27 in Amendment 003.

Question 90:

Do we need a completed PSOS or DOS prior to responding to this tender or, if we're not currently registered, is that process initiated in the event a contract is awarded?

Answer 90:

The Bidder must hold the required security clearances prior to bid closing. Please refer to Part 6 – Security and Other Requirements, article 6.1 and Part 7 – Resulting Contract Clauses, article 7.4.

Question 91:

At APPENDIX 2 to ANNEX A – Key Activities on page 4 of 6 item (b) identifies the need to “Deliver Access Control and User Management Plan” however such a plan requirement is not identified as a SOW requirement in SECTION 5: IT SECURITY REQUIREMENTS even though the Crown references a number of access control requirements in Access Control and Account Management (SC.01, SC.02, SC.03). Does the Crown require a distinct deliverable from the other SA&A deliverables identified on page 39 of 70 of ANNEX A – Statement of Work, and if so what is the Table of Contents of such plan?

Answer 91:

As per SC.02, the GC requires documentation indicating the access controls and associated roles which will satisfy the business requirements as described in, but not limited to: APP-AU.03 APP-OPS.01-.23, APP-IM.05 and APP-IM.07.

A new requirement has been added to Section 5, IT Security Requirements to clarify the deliverable required. Please see Change 64 in this Amendment.

Question 92:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.47 (page 48 of 70). The Contractor must provide Operational Security Procedures to GC that includes, at a minimum:

(a) For each Privileged User role:

- i. Schedule of security-relevant actions to be performed in order to maintain the security posture of the ISS;
- ii. How to use available operational interfaces; and
- iii. Each scheduled action and how the User is expected to perform it.

(b) Operational roles and responsibilities for:

- i. Interaction requirements with PWGSC representatives;
- ii. **Reporting schedule and procedures;**
- iii. Access control;
- iv. Audit and accountability;
- v. Identification and authentication;
- vi. System and communications protection;
- vii. Awareness and training;
- viii. **Configuration management;**
- ix. **Contingency planning;**
- x. **Incident response;**
- xi. Maintenance;
- xii. Media protection;
- xiii. **Physical and environment protection;**
- xiv. **Personnel security;** and
- xv. System and information integrity.

Question:

Operational Security Procedures are always the responsibility of the IT operating authority and require a detailed knowledge of the IT operating authority's organization, policies, standards and management/operating procedures.

Will Canada please confirm/clarify the Bidder's responsibilities in this regard?

Answer 92:

The Contractor is responsible to develop both operational and systemic processes as part of the solution. Therefore the Contractor must document the operational procedures that support the day to day operation by both Internal and External Users for all roles within the Solution. For any Solution processes that are to be effected by PWGSC CIOB and/or SSC, the Contractor will work with the GC to ensure that

the processes are understood and sufficiently documented to minimize operating errors. The procedures must take into account all relevant security requirements to ensure that user errors result in minimal additional risk to Canada.

Question 93:

In reference to Annex A – Statement of Work, Section 3: Technical Requirements, 1.2 Technical Requirements, Tech.19 (page 33 of 70):

Could the response or acknowledgement be outside the portal solution (ex.: email)?

Answer 93:

Tech.19 refers to scalability not messaging. With respect to the Bidders question, not all communications/notifications to the external user is to remain within the Solution. Emails notifications are to be sent to the external user notifying of an ISS communication that requires the external user to access the Solution to retrieve the message.

Question 94:

If we will be responsible for providing additional reporting options such as reports and dashboards, will they be expected to be developed in Business Objects? What version of Business Objects is currently installed at the client site?

Answer 94:

Business Objects will be available in the event that the Contractor identifies that CRM is not capable of providing all required reporting functionality. Regardless, the solution must be configured to link to Business Objects to allow for reporting flexibility should there be a need to expand beyond CRM's capabilities in the future as a part of the solution's sustainment/scalability (Tech.15, Tech.16 and Tech.19).

The version of Business Objects that is currently available includes the following:

- SAP Business Objects BI Suite 4.0 (sp.2)
- Netweaver Business Warehouse 7.3
- Netweaver Foundation for Third Party Apps 7.3
- SAP Business Objects Text Analysis XI 3.0 (SP.2)
- Text Analysis Language Processing (all other languages except Finnish)
- SAP Business Objects Planning & Consolidation for the Public Sector 10.0

Question 95:

SOW NUM SC.09 - The current list of 3rd Party Service providers of external information system services as identified in Figure 2: High level ISST Solution architecture diagram on page 30 of the RFP lists the following: SABA, Electronic Procurement Solution (EPS), Canada Post Address Validation, Credit Bureau's, RCMP, CSIS, and ISS Finance Reviewer General Buy Button (RGGB).

The Contractor assumes the requirement above only applies to non-federal government entities, namely SABA, Canada Post Address Validation provider, and Credit Bureau's. Please confirm this assumption is correct.

Answer 95:

With respect to requirement SC.09, the requirement refers to all the other applications outside of the ISST Solution (MS Dynamics CRM 2015 or higher and its components) that need to connect to the ISST Solution, whether they are external to government or other internal to government applications.

As an example, the SABA application is a learning management platform and is considered a non-government solution. SABA will serve 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. The solution must have the ability to ingest updates from SABA pertaining to completed training in order for service requests to be processed.

For additional information regarding the ISST Solution interfaces please refer to the responses to Question 16 in Amendment 003 and Question 65 in Amendment 006. The GC would also like to indicate that Figure 2 has been removed for revision due to changes in the Business Needs for Security and the Solution's security profile (Please see response to Question 35 in Amendment 003).

Please also refer to Change 61 and Change 65 in this Amendment, both of which are in relation to SABA.

Question 96:

Annex A – Statement of Work, section 3 (Technical requirements), subsection 1.1 (Requirement Overview) - The graphic shows that MS Dynamics CRM for Outlook will be utilized by the Field Inspectors to submit and retrieve information.

- a) Will all the field inspectors have workstations to utilize MS Dynamics CRM of Outlook or is there an expectation of Mobile device support which would require a different connection method?
- b) If Mobile device support is required, will the graphic be updated to include the mobile device requirements, or is the expectation that this will be vetted during the Planning and Analysis process?

Answer 96:

With respect to the requirement for MS Dynamics CRM for Outlook, the ISS Inspectors/Investigators will use their Government Furnished Equipment (GFE) notebooks to utilize MS Dynamics CRM for Outlook. No other requirement for mobile device support for this type of off-line capability/functionality has been identified.

Question 97:

Regarding the Implementation of the solution - The requirements are to complete a Pilot and then conduct a Phased Roll-out.

- a) What is the desired composition of the Phased Roll-out?
- b) How many phases are anticipated?
- c) What is the scope of each phase, i.e., will a phase encompass a sub-set of users or data or cases?
- d) Will roll-out from a specific system constitute a phase?
- e) If roll-out from a system is to be in more than one phase, what is the requirement to maintain data on two systems concurrently or to split the roll-out to only migrate a portion of the data in each phase. Will ISS be responsible for any required system changes in the originating system related to a phased roll-out and data migration?

Answer 97:

The phased roll-out approach is required to ensure that the Solution can be deployed in a controlled fashion to minimize impact both externally and internally to the ISS.

- a) The desired composition of the phased roll-out is one where business activities (e.g. Submission of Security Requirements Check List (SRCL), or Organization Registration with the ISS, etc.) are

released into production one at a time or within logical groupings until the full Solution has been implemented.

- b) The Contractor should recommend the number of phases within their Solution Delivery Plan. The plan would be subject to the approval of the Project Authority.
- c) The scope of the each phase ensures that business activities are released in their entirety to ensure smooth adoption. If, for example, a component of the organizational registration activity could not be rolled out due to an incomplete system plugin, then the remaining components of organizational registration should wait until that plugin has been completed.
- d) A phase should consist of the roll out of an entire business line (all business activities linked to a program) and the technology that supports it.
- e) Details regarding how the data will be handled during the phased roll outs have yet to be determined. The Contractor should provide a proposed recommendation within their Solution Delivery Plan.

Question 98:

Data Migration – What is the expectation for Data Cleansing as related to the Data Migration? Is there an expectation for automated data cleansing? If data cleansing is to be manual, please confirm that this is the responsibility of ISS.

Answer 98:

The Project Authority is responsible for data cleansing. The Contractor is responsible for data migration planning, development, and validation using a controlled sample of data that will be provided by the Project Authority. For additional information regarding the scope of the data migration, please refer to the response provided to Question 87 in this Amendment.

Question 99:

Tech.20 – Please define what, exactly, is the acceptable response time (near real time).

Answer 99:

The solution should be responsive while being able to handle transaction diversity and volumes as identified in the SOW. With respect to Tech.20, we define real time as being within 5 seconds after required processing has completed. An acceptable response time will be determined between the Contractor and Project Authority post contract award.

Question 100:

P. 55 of Annex A – TM.09 and TM.10 – “The contractor must (d) ensure testing cycles continue until a full cycle is completed without any new bugs or defects.” Please specify precisely the severity level of bugs/defects that are included in this requirement. Does this include bugs/defects considered to be Minor or Trivial?

Answer 100:

The Contractor must continue testing cycles until all bugs and defects have been addressed to the satisfaction of the Project Authority. It is expected that the contractor will raise bugs and defects prior to engaging in a testing cycle to confirm necessary action. The Project Authority will only consider excluding bugs and defects from a particular testing cycle under exceptional circumstances, and on a case by case basis. Should a bug or defect be identified for exclusion from the testing cycle by the Project Authority, then it will not need to be addressed for that cycle. Once bugs/defects are addressed to the satisfaction of the Project Authority, then that testing cycle will end.

Question 101:

P. 55 of Annex A – TM.11 – “Contractor must conduct Data Validation testing...of data received from the legacy systems into the new solution”. Please clarify what data this includes as this appears to conflict with the statement that ISS will conduct the Data Migration.

Answer 101:

With respect to TM.11, the bidder will be responsible for migrating a cleansed representative sample of data that will be provided by the Project Authority. The Contractor will be required to perform validation testing on the migrated sample of data to ensure the accuracy of developed migration scripts. The actual data migration will be performed by the Project Authority utilizing the Contractor developed migration scripts. Please refer to data migration requirement APP-DM.04.

Question 102:

Training – please clarify expectations as to completion of training: Is all training required to be completed prior to production go-live or is it to be completed prior to roll-out. Both requirements are stated in the RFP.

Answer 102:

The Contractor must ensure that training is provided incrementally, and recursively, such that External and Internal users are fully trained and able to use each successive roll-out of the Solution upon release. To restate what is written in the RFP, training is to start as early as possible, be recursive and targeted to audiences prior to the planned pilot phase and subsequent incremental roll-outs.

Question 103:

APP.ICN.10 “Interfaces with DND’s Director Foreign Liaison system.....Note that this requirement may change to become a requirement to interface with the US Department of Defence, Defence Security Service System, if possible” Please confirm that this represents two separate requirements that must be estimated for in the response.

Answer 103:

Requirement APP-ICN.10 will be removed from the RFP. Please see Change 62 in this Amendment.

Question 104:

Please confirm that “project closeout” and “contract closeout” have been used interchangeably at M1 and M2:

- M1: Detailed project description must include: iv. Budget management (including the overall cost of services contracted for both at contract award and at project closeout);
- M2: Detailed project description must include: iv. Budget management (including the overall cost of services contracted for, both at contract award and at contract closeout);

Answer 104:

The Crown acknowledges that the terminology “project closeout” and “contract closeout” have been used interchangeably at M1 and M2. To provide clarity for the requirement of budget management evaluation criteria M1 has been amended from “project closeout” to “contract closeout” to maintain consistency. Please see Change 66 in this Amendment.

Question 105:

At M2, please confirm that the words “Reference Project” at the end of the first paragraph at M2 should not actually appear.

Answer 105:

Please note that M2 was amended previously. See Changes 51, 52, and 53 in Amendment 004.

Question 106:

At R1, “Project Management” can be interpreted to require six (6) separate documents and plans (for criteria A through F) in addition to the preliminary Project Management Plan. Please confirm that Bidders’ responses to R1 “Project Management”, A through F, is a single preliminary Project Management Plan.

Answer 106:

The Crown confirms that both a Preliminary Project Management Plan and Project Management Plan are required. Criteria A through F should be included as components of the Project Management Plan and are not separate requirements.

The wording of Technical Evaluation, R1, Criteria A has been amended as the Project Governance and Team Structure is a component that should be included in the Project Management Plan but does not necessarily have to be a stand-alone document.

Please see Changes 67 – 71 in this Amendment.

Question 107:

At Annex A, SAAG.02 (page 39) & SC.18 (page 44) – The acronym “SDSD” is used twice; however, it appears to have 2 meanings. In SAAG.02 it reads “Security Detailed **Solution** Design (SDSD)” and in SC.18 it reads “Security Detailed **Service** Design (SDSD)”.

As these terms are different, yet use the same acronym, please confirm whether these are the same deliverable or are they distinct deliverables

Answer 107:

The deliverables identified as “Security Detailed Solution Design (SDSD)” and “Security Detailed Service Design (SDSD)” at SAAG.02 and SC.18 respectively, are one and the same, and should be referred to as the Security Detailed Solution Design. Please see Change 63 in this Amendment, where the wording of SC.18 has been corrected.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME