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.** 008
Client Reference No. - N° de référence du client 20170549	**Date** 2017-08-04
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** 2017-08-25	**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 008

Purpose:

A. To identify changes to the (Request for Proposal) RFP.
B. To provide answers to questions received with regards to this RFP, and to extend the closing date to August 25, 2017.

A. CHANGES

Change 72:

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.1 Requirement Overview – Functional Requirements, **DELETE** item (k) in its entirety and **REPLACE** with the following:

(k) Facilitates reporting on ISS business activities and trends through available reports; and

Change 73:

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.1 Service Processing Application:

INSERT:

APP-OPS.25	Provides unique identifiers to system objects such as cases and companies that can be viewed and referenced by internal and external clients.

Change 74:

At ANNEX A, SECTION 2: BUSINESS REQUIREMENTS, under 2.2.2 Web Portal, **DELETE** WP-UE.11 in its entirety and **REPLACE** with the following:

WP-UE.11	Provides access to downloadable fillable forms that must contain the same data fields as their online counterparts for user completion.

Change 75:

At ANNEX A, SECTION 3: TECHNICAL REQUIREMENTS, under 1.1 Requirement Overview:

DELETE:

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.

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 High Level ISST Solution Conceptual Architecture and 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.

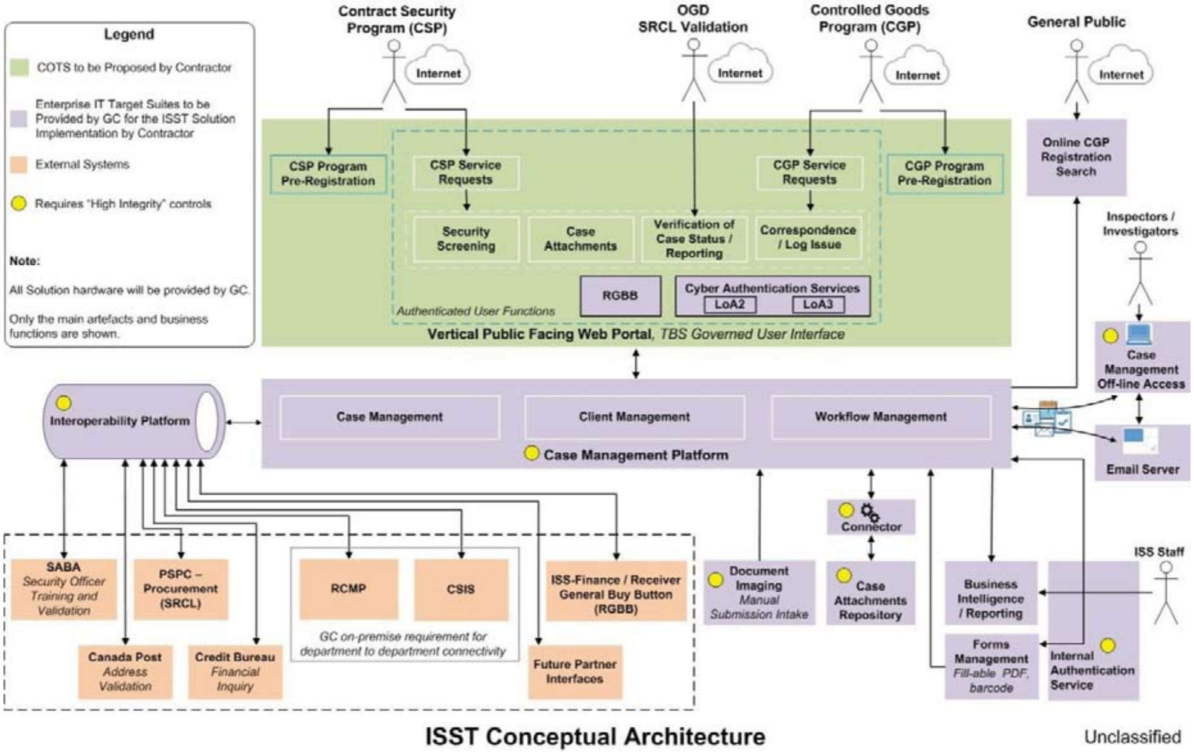
Legend
🟩 COTS to be Proposed by Contractor
🟪 Enterprise IT Target Suites to be Provided by GC for the ISST Solution Implementation by Contractor
🟧 External Systems
● Requires "High Integrity" controls
Note:
All Solution hardware will be provided by GC.
Only the main artefacts and business functions are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

Figure 2: High Level ISST Solution Conceptual Architecture

Change 76:

At ANNEX A, SECTION 3: TECHNICAL REQUIREMENTS, under 1.2 Technical Requirements:

INSERT:

Tech.39	Provide a Solution that allows for the management of forms via configuration in Dynamics (or another means) without the need of a developer.
Tech.40	Design the solution to ensure that "digital signatures" are used for both, internal user and internal service initiated processes where required.
Tech.41	Identify and describe, within their physical architecture design, the security controls to be implemented by the Contractor, and the GC.
Tech.42	Define the contents for and configure the solution to produce system generated audit files to include information to facilitate integrity violations determination.
Tech.43	Configure the solution to enforce user account restrictions (e.g. time of day, day, week, etc.)
Tech.44	Create a process that will store previous configurations of the solution to support version rollback for a period to be defined by the GC.
Tech.45	Configure the solution to prevent unauthorized and unintended information transfer via shared system resources.

Tech.46	Configure the solution to respond automatically when integrity violations occur.
Tech.47	Purchase and configure a COTS web Portal technology that meets the requirements of the current solicitation.

The Contractor must provide a COTS Web Portal technology that:

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

Change 77:

At ANNEX A, SECTON 4: SECURE ACCESS, under 1.2.1 Internal Users:

INSERT:

SecureInt.07	Uses digital signatures for Internal Users related processes where required.

Change 78:

At APPENDIX 2 TO ANNEX A – KEY ACTIVITIES, at the end of the first paragraph, **INSERT** the following:

Delivery dates for the project milestones will be subject to contract award and start date of the contractor. Should delays occur in the awarding of a contract, project milestone dates will be adjusted accordingly. Adjustment of timelines, if required, will occur upon contract award.

Change 79:

At Attachment 1 to Part 4 – Technical Evaluation, 1. Overview of the Technical Evaluation, at the end of the first paragraph, **INSERT** the following:

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

Change 80:

At Attachment 1 to Part 4 – Technical Evaluation, 1. Overview of the Technical Evaluation:

DELETE:

Technical Evaluation Summary			
ID	**Mandatory Criteria**		**Met/Not Met**
M1	Corporate Reference Projects: Business Process Re-engineering and Change Management		
M2	Corporate Reference Projects: IT Solution		
M3	Customer References		
ID	**Point Rated Criteria**	**Maximum Points**	**Actual Score**
R1	Project Management	620	
R2	Business Process Re-engineering	360	
R3	Relationship Management	160	
R4	Security Management	360	
R5	Sensitive Data Migration	200	
R6	Change Management Plan	380	
R7	Testing Plan	160	
R8	Corporate Reference Projects: Government of Canada Client	80	
R9	Corporate Reference Projects: Case Management and Microsoft Dynamics CRM	180	
Maximum Total Points for Point Rated Criteria		**2500**	
Minimum Pass Mark for Point Rated Criteria (70%)		**1750**	

INSERT:

<table>
<tr><th colspan="4">Technical Evaluation Summary</th></tr>
<tr><th>ID</th><th colspan="2">Mandatory Criteria</th><th>Met/Not Met</th></tr>
<tr><td>M1</td><td colspan="2">Corporate Reference Projects: Business Process Re-engineering and Change Management</td><td></td></tr>
<tr><td>M2</td><td colspan="2">Corporate Reference Projects: IT Solution</td><td></td></tr>
<tr><td>M3</td><td colspan="2">Corporate Reference Projects: COTS Solution</td><td></td></tr>
<tr><td>M4</td><td colspan="2">Customer References</td><td></td></tr>
<tr><th>ID</th><th>Point Rated Criteria</th><th>Maximum Points</th><th>Actual Score</th></tr>
<tr><td>R1</td><td>Project Management</td><td>620</td><td></td></tr>
<tr><td>R2</td><td>Business Process Re-engineering</td><td>360</td><td></td></tr>
<tr><td>R3</td><td>Relationship Management</td><td>160</td><td></td></tr>
<tr><td>R4</td><td>Security Management</td><td>360</td><td></td></tr>
<tr><td>R5</td><td>Sensitive Data Migration</td><td>200</td><td></td></tr>
<tr><td>R6</td><td>Change Management Plan</td><td>380</td><td></td></tr>
<tr><td>R7</td><td>Testing Plan</td><td>160</td><td></td></tr>
<tr><td>R8</td><td>Corporate Reference Projects: Government of Canada Client</td><td>80</td><td></td></tr>
<tr><td>R9</td><td>Corporate Reference Projects: Case Management and Microsoft Dynamics CRM</td><td>180</td><td></td></tr>
<tr><td>R10</td><td>COTS Web Portal Solution</td><td>220</td><td></td></tr>
<tr><td colspan="2"><b>Maximum Total Points for Point Rated Criteria</b></td><td><b>2720</b></td><td></td></tr>
<tr><td colspan="2"><b>Minimum Pass Mark for Point Rated Criteria (70%)</b></td><td><b>1904</b></td><td></td></tr>
</table>

<u>**Change 81:**</u>

At Attachment 1 to Part 4 – Technical Evaluation, 3. Mandatory Criteria, M2:

DELETE:

E. For at least one (1) Reference Project, the solution implemented must have had security requirements similar to those identified in ANNEX A, Section 5, 1.2 IT Security Requirements.

<u>**Change 82:**</u>

At Attachment 1 to Part 4 – Technical Evaluation, 3. Mandatory Criteria, M2:

INSERT:

G. For at least one (1) Reference Project, a COTS web portal product must have been implemented and integrated with a COTS application. The solution must have had security requirements similar to those identified in ANNEX A, Section 5, 1.2. IT Security Requirements. For the purpose of this evaluation, similar IT security requirements would be defined as having implemented a solution that uses sensitive data (Protected B) and requires the protection of data integrity.

Change 83:

At Attachment 1 to Part 4 – Technical Evaluation, 3. Mandatory Criteria:

DELETE

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

INSERT

M3	**Corporate Reference Projects: COTS Solution** The Statement of Work identifies the requirements for the COTS web portal technology. The bidder must provide a full description of the COTS web portal technology that will be installed on GC premises including: A. Product and version; B. Server requirements; C. Database requirements; and D. Integrability with MS Dynamics (on-premises) 2015 or higher. The response must also demonstrate that the proposed technology has the ability to meet the requirements referenced in Sections 2, 3 and 4 in Annex 1.	
M4	**Customer References** For each Reference Project provided in response to M1, M2 and M3, the Bidder must complete Form 2 to Part 4. The client contact may be contacted to validate the information provided in the Bidder's response, in accordance with Part 4.2.4, Reference Checks.	

Change 84:

At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria R3:

DELETE

Maximum Points : 170

INSERT

Maximum Points : 160

Change 85:

At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria R7:

DELETE

Maximum Points : 170

INSERT

Maximum Points : 160

Change 86:

At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria:

INSERT

<table>
<tr>
<td><b>R10</b></td>
<td>
<b>COTS Web Portal</b>
Based upon the COTS Web Portal technology proposed in response to M3, the Bidder should indicate whether portal technology has been successfully implemented in other solutions, whether it has a licensing model and if it has out of the box functionality to meet requirements in the SOW, or requires functionality built in and would require additional configuration.
A. The Bidder should demonstrate that they have successfully implemented the portal technology in other Reference Projects. Bidders are requested to complete Form 2 to Part 4 for all Reference Projects provided in response to R10. The client contact may be contacted to validate the information provided in the Bidder’s response, in accordance with Part 4.2.4, Reference Checks.
B. The Bidder should describe the proposed licensing model including renewal, support and software assurance. The licensing model should be submitted in order to obtain points for this criteria.
C. The Bidder should complete the following table by placing an X in the appropriate column, to indicate whether the requirement will be met by the Web Portal Technology proposed in response to M3 out of the box (OB), or if it will require configuration (RC):
</td>
<td>
<b>Maximum Points : 220</b>
Part A Maximum Points : 30
<table>
<tr><th>Number of Projects</th><th>Points</th></tr>
<tr><td>0</td><td>0</td></tr>
<tr><td>1-5</td><td>20</td></tr>
<tr><td>6+</td><td>30</td></tr>
</table>
Part B Maximum Points : 25
<table>
<tr><th>Licensing Model</th><th>Points</th></tr>
<tr><td>Detailed Licence Model (DLM)</td><td>5</td></tr>
<tr><td>DLM + Renewal (R)</td><td>10</td></tr>
<tr><td>DLM + R + Support (S)</td><td>15</td></tr>
<tr><td>DLM + R + S + Software Assurance</td><td>25</td></tr>
</table>
Part C Maximum Points : 165
<table>
<tr><th>COTS Config-uration</th><th>Points per requirement</th></tr>
<tr><td>Out of the box (OB)</td><td>15</td></tr>
<tr><td>Requires configuration (RC)</td><td>0</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

COTS Web Portal Requirements	Out of the box (OB)	Requires configuration (RC)
Must conform to GC Web Standards and Web Accessibility (Tech.18)		
Enables secure access at logon by supporting multi-factor authentication capability (WP-SH.01)		
Will support 1000 concurrent users (WP-SH.03)		
Language Preference: Application External User interfaces must be available and presented in the user's Official Language of choice. (WP-UE.25)		
Provides form validation as each section is completed with clear and concise message to alert the External User to potential errors (WP-UE.21)		
Has search capability (WP-SH.12)		
Enables portal user self-service by exposing any pre-configured or customized Dynamics CRM form through the web portal (Tech.12)		
Enables External Users to save their submitted forms to PDF format (WP-UE.20)		
Enables External Users to use common mobile devices that are equipped for Internet browsing to access the web portal at any time using any device. This includes electronic signatures (WP-UE.05)		

		Is configured to connect to Microsoft Dynamics CRM 2015 or higher (Tech.12)					
		Supports scalability (Tech.19)					

B. QUESTIONS

Question 108:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.33 (page 46 of 70). The Contractor must report all suspected or actual privacy and security violations as security Incidents for the duration of the contract.

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

Answer 108:

The Contractor is responsible for security monitoring of the Solution (non-infrastructure), access to the Solution, and the Solution data for the duration of the contract. This includes inappropriate access by GC staff and Contractor, intentional or accidental. All such incidents must be reported to the appropriate authority.

Question 109:

In reference to Attachment 1 to Part 4 – Technical Evaluation, Section 3. Mandatory Criteria, M2, E. (page 5 of 10), the RFP states “For at least one (1) Reference Project, the solution implemented must have had security requirements to those identified in ANNEX A, Section 5, 1.2. IT Security Requirements;

We respectfully suggest that this requirement be amended as follows “For at least one (1) Reference Project, the solution implemented must have had security requirements **similar** to those identified in ANNEX A, Section 5, 1.2. IT Security Requirements.” Could, PSPC, please, also clarify what level and extent of demonstration of similarities are required?

Answer 109:

Technical Evaluation M2 has been amended to remove Item E. Please see Change 81 in this Amendment.

Question 110:

To what degree is the supplier allowed using tools/platforms that reside outside of the on-site ISST delivery environment (e.g. public or private cloud) to support the delivery of the initiative?

Answer 110:

The Contractor will only have access to the delivery environment until the completion of the vulnerability assessment and readiness assessment of the production environment.

Additionally, as indicated within the SRCL part C, where the Contractor is required to access Protected or Classified information or assets, the Contractor is required to do so on GC premise and is required to utilize GC IT systems. The Contractor is not permitted to receive or store Protected or Classified information or assets on their site or premise, nor can the Contractor use its own IT systems. In addition no electronic link will be provided between the GC and Contractors IT systems.

Question 111:

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

Answer 111:

In June 2013 a data quality analysis was performed on a portion of the ISS data supporting Contract Security Program while the remainder was analyzed in September 2015. The Project Authority is currently in the process of reviewing that analysis and is to start data cleansing on portions of the data prior to contract award. All information gathered during the analysis will be provided to the bidder post award.

Question 112:

On page 56 of 70 in the Statement of work item b) of PWGSC's responsibilities, the Crown indicates it is responsible to "Review of deliverables and the provision of feedback and approvals in a timely manner".

a) Is the Crown committed to reviewing deliverables and providing written feedback for simple to medium level complexity deliverables within 5 working days?
b) Is the Crown committed to reviewing deliverables and providing written feedback for complex level deliverables within 10 working days?

Answer 112:

Timely manner will be determined by the Contractor and Project Authority after the contract has been awarded.

Question 113:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.21 (page 45 of 70). The Solution must:

a) Protect information in transit between systems;
b) Protect information at rest in the system; and
c) Provide the functionality to integrate cryptographic solutions in accordance with CSE recommendations and TBS policies.

Question/Comment:
a) Do you require file-level encryption?
b) Will Canada provide suitable encrypted data storage devices?
c) Will Canada provide a suitable Key Management System?

Answer 113:

With respect to SC.21:

a) No, disk level encryption is required. MS Dynamics as deployed within the GC, encrypts by tenant at the disk level.
b) Canada will provide suitable encrypted, data storage devices.
c) The Contractor will leverage the existing key management system that is currently deployed within the GC.

Question 114:

At ANNEX A – Statement of Work, requirement SC.34 under Incident Management, the Crown requires that “The Contractor must provide support and assistance to the GC in implementing mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, and removing malicious malwares) to contain a Security Incident and to protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada’s priority level for the duration of the contract”.

The firewalls and Intrusion Detection and Prevention appliances are core security infrastructure components normally under Shared Services Canada (SSC) responsibility.

Understanding that the initial contract period of 29 months may be extended by up to four (4) additional six (6) month period(s) under the same terms and conditions, the contractor requires specialized security personnel to support the implementation of firewall rules and IDS/IPS signatures. However, the Crown has not identified any security personnel categories in its rate card for “As-and-When-Requested Work”.

a) Will the Crown add such security personnel category (e.g. Network Security Analyst) to support as and when security incidents occur?
b) In addition since the Contractor cannot submit a proposal with assumptions, will the Crown specify the characteristics of its firewall(s) and IDS/IPS appliances in order for the Contractor to have such qualified personnel on hand should an incident occur? Firewall and IDS/IPS appliance characteristics would be at least vendor name, model and version number.

Answer 114:

a) The GC will not add a security personnel category to the "As-and-When-Required” section of the RFP. The RFP clearly states security requirements including a need for high integrity implementation. The Contractor should develop their approach to the Solution accordingly. Please also refer to the response provided to Question 120 in this Amendment 008.
b) For security reasons, the GC will not provide any details regarding the configuration or identification of public facing GC firewalls or any other network device in a public forum. The successful bidder will receive relevant information upon contract award.

Question 115:

In reference to Annex A – Statement of Work, Section 3: Technical Requirements, 1.2 Technical Requirements, Tech. 33 (page 35 of 70):

In which phase should the Protected B level be applied to the database (development process or production phase)?

Answer 115:

All Production data/information must be accordingly protected as per Tech.31. Should the contractor require production type data/information for development purposes, all production type data/information supplied for this purpose must be masked.

Question 116:

Re-estimation may be required in cases where the re-engineering process eliminates and/or creates additional TARGET data sources, will we be able to revise estimates if this arises?

Answer 116:

The Bidder should account for the potential expansion of target data sources and any other risks related to deliverable work covered within the RFP as a part of their bid price within their bid proposal using the provided business process maps and business processing re-engineering requirements. The Bidder should outline their methods for approaching these risks in the technical evaluation response to Rated Criteria R1.

Question 117:

Since we will be estimating prior to the execution of the process re-engineering which will conceivably change the TARGET data matrix, will we be able to revise estimates (possibly increase time and cost) after the process re-engineering is complete?

Answer 117:

Please see response to Question 116 in this Amendment 008.

Question 118:

In reference to Data Storage:

a) With regard to the source data for the migration, are any of the 6 identified systems storing data in either a PUBLIC or PRIVATE cloud environment?
b) With regard to the source data for the migration, are any of the 6 identified systems storing data in a SAN environment?
c) With regard to the new target data delivered by the migration, are there plans to store the CRM database in a PUBLIC or PRIVATE cloud, or in a SAN environment?

Answer 118:

With respect to Data Storage:

a) ISS source data is currently on a GC private servers environment, SSC hosted.
b) ISS environments are virtualized and the VM hosts are using SAN to store the data.
c) The location of the target environment for the data is dependent upon the ability to host PB/H/M information. The Dynamics application is on-premise and will be the data repository. Public cloud is not under consideration.

Question 119:

Is the BI environment an ensemble of a data warehouse and data marts (Inmon configuration), or only data marts (Kimball configuration)? If it is an Inmon configuration are there one or many data warehouses?

Answer 119:

Currently there is no BI environment for the ISS or the ISST project.
The version of Business Objects that is currently available within PWGSC 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

Please refer to Question 94 in Amendment 007 for additional information regarding business objects.

Question 120:

Form 3 to part 4 Section 3 table 2 “As-and-when-requested work” identifies rates for 9 resources at level 3. Reviewing these resources against SOW Section 9 shows that roles for Business Process Reengineering, Testing, Project Management, Change Management and Solution Sustainment are not included in the rate table. Further Section 9 does not include design resources (e.g. architect/modeler) for analytics. Can you indicate if only the 9 resources at level 3 are to be provided (if yes then please indicate how the missing resource classes would be addressed), if vendors should add rows to the table or if the table will be amended to include missing resource classes?

Answer 120:

For the purpose of financial evaluation of bids, the bidders only have to provide the 9 resources at level 3 as requested in the RFP. After contract award, should it be determined that new resource categories are necessary for the requirement, please refer to Part 7 of the RFP, Resulting Contract Clauses, section 7.1 Requirement, item (e):

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

Question 121:

Would Canada please confirm that the rate card, based on 120 days across 9 roles, is not included within the financial cap of $11M?

Answer 121:

Section 2. Firm Lot Price of the Financial Bid Form states: “The Total Firm Lot Price must not be less than $6,000,000.00 and must not exceed $11,000,000.00.”

The Total Firm Lot Price is the total price for all milestones requested in Table 1 – Firm Lot Price and Milestone Schedule. It does not include any of the costs for As-and-when-requested work. Therefore the amounts and costs in Table 2 are not subject to the $11M limit.

Question 122:

SOW NUM SC.22 - The entry and exit points to the solution as shown in Figure 2: High level ISST Solution architecture diagram on page 30 of the RFP are the Internet Enrolment and Registration Portal, the Case Management Platform to the GC Interoperability Platform (Oracle BPM Suite), Imaging / Scanning Systems, Document and Records Management System, Forms Management and ETL interfaces as well as the MS Exchange Server. These entry points should already be protected by PWGSC security platforms from malicious code infiltration.

Please confirm the Crown wishes the Contractor to provide malicious code protection mechanisms in addition to existing PWGSC / SSC security technologies in place?

Answer 122:

Platform/infrastructure malicious code protection is normally installed, supported and managed by SSC and or PWGSC. The Contractor is responsible to ensure that if protection or additional protection is required within the application level, in accordance with the stated security controls, then the Contractor must apply the approved and appropriate malicious code protection.

Question 123:

SOW NUM SC.27 - Is the security assessment plan a different deliverable than the SAAG.03 - (f) Vulnerability Assessment Plan as both refer to the management of vulnerabilities?

Answer 123:

The Security Assessment Plan (SAP) is a different deliverable from the Vulnerability Assessment Plan (VAP) but they are related. While the SAP is an overarching document covering all security aspects of the solution, the VAP may be an element of the SAP focusing on known or revealed vulnerabilities. Where the SAP will not contain significant details regarding the vulnerabilities, the VAP must include fine details. Both are evidence documents required for SAAG certification.

Question 124:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.22 (page 45 of 70).

(a) Employ malicious code protection mechanisms at entry and exit points to the Solution that can detect and eradicate malicious code;

(b) Maintain the malicious code protection mechanisms in an up-to-date state in accordance with organizational configuration management policies; and

(c) Use mobile code only in ways that are fully documented and maintain the other security protections in the solution.

Question/Comment

(a) Can it be assumed that anti-malware protection at network zone boundaries would be provided by SSC as part of the host environment? If so, would the bidders only be responsible for local/host-based malware protection within the solution itself?
(b) Operational COTS system updates (other than bidder custom code) would normally be the responsibility of the IT operating authority. Please clarify.

(c) Can you please confirm that the bidder is not responsible for operational updates and patches for COTS products?

Answer 124:

Malicious code protection at network zone boundaries is the responsibility of SSC. The Contractor is responsible for any solution application based malicious code protection required/configured within the solution. The Contractor will be responsible for solution component code protection, patches and updates including COTS products, implementing them through service tickets and PWGSC IT Change processes, once solution is released in production and for the duration of the contract.

Question 125:

Project Implementation PM.16 "The Contractor must provide a proposed Solution Delivery Plan that appropriately addresses requisite activities and deliverables, respects the overall timeline of the project, anticipated phased rollout approach and recursive communication, testing and training cycles. Identified deliverables within the Solution Deliver Plan should be reflected in the Project Schedule and Change Management activities. The Solution Delivery Plan should also align with the Key Activities outlined in APPENDIX 2 To ANNEX A."

PM.16 identifies a deliverable called a Solution Delivery Plan. Please clarify the intent and scope of this Plan. It appears that this is a specific plan for the delivery of the solution into Production, AFTER the completion of initial User Acceptance Testing. Does this plan include the Pilot Release? It also appears that this plan is intended to include re-testing of the application after completion of the Pilot.

Please confirm all of the above or provide a Table of Contents for this deliverable.

Answer 125:

The Solution Delivery Plan speaks to all of the delivery phase, it does not end after the pilot. The Solution Delivery Plan is to include how the Contractor intends to deliver on the various aspects and components of the Solution as outlined in PM.16. The Solution Delivery Plan is to cover the period from planning to the point of implementation of the Solution. For more information regarding the Solution's pilot and phased rollout please see the response to Question 97 in Amendment 007.

Question 126:

With respect to Annex A, Section 2.1, Item (k) – Please quantify/identify how many reports (if any) are expected to be created/re-created/implemented by the Contractor as part of the proposed reporting solution.

Answer 126:

The Contractor is expected to develop functionality that will provide the Project Authority the flexibility to create and modify reports that will be made available to the ISST users (External and Internal). Please refer to the Reporting and Analysis requirements provided in Section 2, 2.1 Business Requirements – Functional Requirements. To clarify the identified concern, the identified item (k) has been amended. Please see Change 72 in this Amendment.

Question 127:

ANNEX A, Section 2: Business Requirements, under 2.2.2 Web Portal states for WP-UE.11: "Provides access to downloadable fillable forms that must contain same data as their online counterparts." Please clarify if the intent of the requirement is for the forms to contain the "same data fields" rather than the same "data values".

Answer 127:
With respect to WP-UE.11 the downloadable forms are to contain the same data fields as the online forms, not any data values. An amendment has been made to WP-UE.11 to clarify. Please see Change 74 in this Amendment.

Question 128:

Can you give us any indication as to when we might expect to see answers to our previous questions? The lack of timely answers to our questions is having a negative impact on our ability to make optimal progress on our bid response.

Answer 128:

GC is committed to responding to Bidders' questions. In order to accommodate the challenges faced by Bidders to complete a bid response, the date of bid closing has been extended to August 25, 2017.

Question 129:

In reference to the RFP, ATTACHMENT 1 TO PART 4 – TECHNICAL EVALUATION, 3. POINT RATED CRITERIA, R4 – Security Management (page 8 of 10), the Bidder's Response instruction contains the following statement: "The Bidder should provide a Concept of Security Operations document which describes an operational scenario for the ISST solution."

Question: Could Canada please clarify by specifying what is meant by an "operational scenario for the ISST solution?" Additional context will help ensure that Bidders know exactly what is required and answer this requirement correctly.

Answer 129:

Please see Change 56 in Amendment 004, which contained an update R4. Included in the Amendment was clarification around what is meant by "operational scenario".

Question 130:

In reference to Amendment 3, Changes 29, 30, 35, 39, 40, 41, and 42 (page 8 of 18); The security posture of the delivered service(s) has been amended from PB/M/M to PB/H/M.

Question: Normally, high integrity (i.e. PB/H/M) is a value assigned to data integrity. Could Canada please confirm that this interpretation is correct and would be adequately achieved by applying certain file-level tamper detection means such as tripwire?

Answer 130:

Yes, the current designation of PB/H/M indicates that the business and system must support operations of a Protected B Confidentiality sensitivity, High Data Integrity and Medium availability. Applying file-level tamper detection may be part of the response to the change. The contractor through the solution design will have the opportunity to include whatever approved devices/methods are required to meet the additional integrity controls added as a result of the integrity change. Please refer to Amendment 003 for additional identified security controls.

Question 131:

As per Amendment 004, Answer 41 – "The Contractor should not assume that GC will provide any software products other than those identified by name in Section 3, Technical Requirements."
SAP Business Objects is identified as a product in section 3.

a) Since SAP licensing has changed in 2016, can the Crown please describe what software components are available under its current licensing plan with SAP?
b) Is SAP Data Integrator available as GFE and if so can the product be deployed in a clustered manner?

Answer 131:

a) The latest SAP contract has the following components:

- 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

b) SAP Data Integrator is not available as a GFE product. The contractor may propose a product as part of their bid. Deployment in a clustered manner would have to be pre-approved.

Question 132:

Given the significance of the changes to the RFP, as well as the large number of outstanding answers to the questions submitted, it is requested that the closing date of the solicitation be extended by a period not less than 4 weeks.

Answer 132:

The date of bid closing has been extended to August 25, 2017.

Question 133:

Attachment 1 to Part 4, M2, F. – Please confirm that a reference project that is fully implemented and in production and that is currently supported/maintained is considered "complete".

Answer 133:

Yes, any referenced project that is fully implemented, in production and is currently being supported/maintained is considered to be "completed" as per Item C, M1 and Item F, M2 of the Technical Evaluation Criteria.

Question 134:

Canada has acknowledged there may be a limited number of government projects that would satisfy M2. Also, security controls must be designed and implemented in same way regardless of volumetric data and diversity of transactions. Therefore, regarding Attachment 1 to Part 4, M2, Item E; we request that the requirement be changed to allow the Bidder to demonstrate experience on a project (not required to be one of the 3 in support of M2) where they have implemented security controls similar to those in Annex A, Section 5, 1.2 – with MEDIUM integrity – to comply with Item E of M2.

Answer 134:

Technical Evaluation criteria M2, Item E has been removed. Please reference Question 109 and Changes 81 and 82 from this Amendment 008.

Question 135:

We kindly request an extension to Aug 31, 2017.

Answer 135:

The date of bid closing has been extended to August 25, 2017.

Question 136:

Please confirm that for purposes of R8, a Government of Canada client includes a corporation incorporated under Part II of the Canada Corporations Act in order to provide services in accordance with federal government Acts and legislation previously provided directly by a government department.

Answer 136:

Government of Canada clients are those defined within the Financial Administration Act (http://laws-lois.justice.gc.ca/eng/acts/f-11/).

Question 137:

With respect to R9:

a) We understood that PSPC had agreed to detach M2 from both R8 and R9. While Amendment 004 detached R8 from M2, it did not detach R9. Please confirm that you will detach R9 from M2.

b) Further, with regards to R9: Sub-section (A) reads like a Mandatory requirement: “At least one of the three reference projects…” Is this intentional?

Answer 137:

Technical Evaluation criteria R9 was updated to no longer be linked to M2 in Amendment 006. Please refer to the response to Question 62 and Change 60 within Amendment 006 for updated information.

Question 138:

In reference to Amendment 006 released on July 19, Change 58 indicates that the score allocation for R3 has been amended as follows:

Delete:

Maximum Points : 170

Part A Maximum Points : 50

Part B Maximum Points : 30

Part C Maximum Points: 40

Part D Maximum Points : 50

Insert:

Maximum Points : 170

Part A Maximum Points : 50

Part B Maximum Points : 25

Part C Maximum Points: 35

Part D Maximum Points : 50

The amended number of maximum points for R3 add up to 160, but still indicates 170. Could PSPC please clarify if this is an error and the total should be 160?

Answer 138:

This was an error and has been corrected in Change 84 in this Amendment. The maximum points for R3 should be 160.

Question 139:

In reference to Amendment 006 released on July 19, Change 59 indicates that the score allocation for R7 has been amended as follows:

Delete:

Maximum Points : 170

Part A Maximum Points: 40

Part B Maximum Points: 100 (Maximum 25 points for each element)

Part C Maximum Points: 30

Insert:

Maximum Points : 170

Part A Maximum Points: 40

Part B Maximum Points: 100 (Maximum 25 points for each element)

Part C Maximum Points: 20

The amended number of maximum points for R7 add up to 160, but still indicates 170. Could PSPC please clarify if this is an error and the total should be 160?

Answer 139:

This was an error and has been corrected in Change 85 in this Amendment. The maximum points for R7 should be 160.

Question 140:

In reference to Annex A – Statement of Work, Section 3: Technical Requirements, 1.2 Technical Requirements, Tech.30 (page 35 of 70): Is the expectation to deploy an instance of the ESB specifically for the use of this initiative, or re-use an existing one within GoC? If re-using an existing one, what are the common existing re-usable services being offered by the ESB that should be considered?

Answer 140:

GC has an established ESB capability and infrastructure. It is in the process of provisioning a domain which is to be leveraged specifically for this initiative. The GC teams will be developing the service interfaces using industry interoperability standards. The Contractor will collaborate with the GC team to confirm service contracts. The Contractor will develop all services necessary within the Case Management Platform, using its supported web services and APIs to make it available for integration by other GC systems. The publication of these services to the ESB will be done by the GC team. These services must be designed and developed using industry interoperability standards, follow SOA best practices, and not depend on vendor-specific or proprietary implementations (e.g., authentication schemes, serialization, object types, semantic models).

Question 141:

We appreciate the flexibility that has been shown in Amendment 3 by de-coupling the reference requirements for M2 and R8. We are curious as to why the same standard was not applied to R9, which still points back to the Mandatory requirement. The requirements for M1 and M2 are significant and stretch back 15 years to a time when MS Dynamics was a very new software package. There would be very few MS Dynamics credentials globally that would meet all the requirements for M2, and thus receive the rated points in R9. Would the Crown please confirm that it would be acceptable for Bidders to include referenced projects in M2 and R8 to respond to the MS Dynamics and Case management requirements in R9.

Answer 141:

Please refer to the response to Question 137 in this Amendment.

Question 142:

Would the Crown please consider granting a three-week extension based on the following criteria:

- Some outstanding questions prohibit us from completing some of our bid response material;
- Changes to M1, M2, R8, and R9 require us to replace some of our previous corporate reference projects therefore delaying the submission of requests for client references approval. Due to time constraints and summer vacations, getting approvals from client references for some of our corporate reference projects are challenging;
- Changes to R4 require us to revise, update, or add information to previously created response material; and
- Changes to several Annex A SOW functional, technical and security requirements impacting some aspects of our delivery approach and technical solution as well as associated pricing, delaying executive review and approvals.

Answer 142:

The date of bid closing has been extended to August 25, 2017.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME