



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

Québec

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

Vendor/Firm Name and Address

**Raison sociale et adresse du
fournisseur/de l'entrepreneur**

Issuing Office - Bureau de distribution

Miscellaneous Special Projects Division (XN)/Division
des projets spéciaux divers (XN)
Canadian Building
219 Laurier Ave. West, 13th Floor
Room 13077
Ottawa
Ontario
K1A 0S5

Title - Sujet e-Procurement Solution (EPS)	
Solicitation No. - N° de l'invitation EN578-131350/H	Amendment No. - N° modif. 025
Client Reference No. - N° de référence du client 20131350	Date 2016-09-22
GETS Reference No. - N° de référence de SEAG PW-\$\$XN-111-30112	
File No. - N° de dossier 111xn.EN578-131350	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM on - le 2016-10-31	
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: Thauvette, Maxime	Buyer Id - Id de l'acheteur 111xn
Telephone No. - N° de téléphone (819) 420-2201 ()	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

Request for Proposal (RFP)**Solicitation Amendment: 025****Purpose:**

The purpose of this amendment is to extend the closing date of this Request for Proposals (RFP), amend the RFP and provide answers to questions received with regards to this RFP.

Canada is currently reviewing possible adjustments to the basis of payment as well as sections related to the implementation of the EPS and, as such, we are extending the closing date of this RFP to October 31st, 2016. Should Canada make substantive changes to these sections, it anticipates an additional extension may be granted to allow Bidders time to review their bids, if applicable. Such an extension would be communicated through a future RFP amendment.

(A) CHANGES**CHANGE: 145**

At Annex 1, section 3.2 *SECTION A - GENERAL REQUIREMENTS*, under *Table 2 - General Requirements*, delete requirement A-01.01 in its entirety.

CHANGE: 146

At Annex 1, section 3.5 *SECTION D - PROCUREMENT MANAGEMENT*, sub section 3.5.6 *Requirements*, delete requirement D-17.03 in its entirety and replace with:

to create multiple Orders from a single Shopping Cart Request based on any data element (e.g. Client, Availability, Dollar Value), including the functionality to:

- i. Send Orders to the appropriate Supplier(s) when there are multiple items associated to a Shopping Cart request from different Suppliers; and
- ii. Provide the User the option of selecting to create an Order based on the lowest overall cost from a single Supplier or the lowest overall cost from multiple Suppliers in accordance with the applicable MOS and Catalogue Attributes (e.g. Order Thresholds, Minimum Order Quantity).

CHANGE: 147

At Annex 1, section 3.10 *SECTION I - DATA AND INFORMATION MANAGEMENT*, sub section 3.10.2 *Requirements*, delete requirement I-06.19 in its entirety and replace with:

for disposition classes to be systematically or manually applied to existing, received or newly created records and associated Metadata, and where applicable, group of records.

CHANGE: 148

At Annex 1 – *Statement of Work*, section 4.3.2.4 *Interoperability with GC Back-Office Systems*, delete:

Functionality to be exposed includes the following:

- a) Ability to create/read/update/delete business objects in the EPS
- b) Ability to invoke/trigger business processes within the EPS
- c) Ability to publish business object and contract lifecycle related events using Near Real-Time messaging

CHANGE: 149

At Annex 1 – *Statement of Work*, section 6.4.2 *Privacy Management Plan delivery*,

DELETE:

The Contractor must provide within 60 business days of Contract Award a one-page awareness training package instructing the Contractor's resources regarding the use of the Personal Information provided by the GC about the Users.

INSERT:

The Contractor must provide within 60 business days of Contract Award a privacy awareness guide instructing the Contractor's resources regarding the use of the Personal Information provided by the GC about the Users.

CHANGE: 150

At *Annex 2 – Security and Privacy*, delete c) in the description of security requirement E2.21 in its entirety and replace with:

c) log events such as database logs, application logs, firewall logs, etc. to allow Canada to identify and assess potential issues; and

CHANGE: 151

At *Annex 2 – Security and Privacy*, delete c) in the description of security requirement E2.23 in its entirety and replace with:

c) Alerting the Contractor's Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and

CHANGE: 152

At *Annex 2 – Security and Privacy*, delete the description of security requirement E2.28 in its entirety and replace with:

The Contractor must develop, document, and maintain under configuration control, a current baseline configuration (N) of the EPS and the previous version (N-1).

CHANGE: 153

At *Annex 2 – Security and Privacy*, delete the description of security requirement E2.29 in its entirety and replace with:

The Contractor must only allow software authorized by the Contractor to execute on the EPS. The software authorization process must be documented by the Contractor.

CHANGE: 154

At *Annex 2 – Security and Privacy*, delete the description of security requirement E2.85 in its entirety and replace with:

The Contractor must provide all evidence associated to a security incident, in a COTS format specified by GC and within a time interval specified by GC, that is associated with GC Data and relevant to the security incident including:

- a) results of historical Application, Network and System logs and audit records research;
- b) results of analysis of Application, Network and System logs and audit records;
- c) Application, Network and System logs and audit records; and
- d) additional clarification information or data as specified by GC based on the review of information provided by the Contractor under items a) to c) above.

CHANGE: 155

At *Annex 2 – Security and Privacy*, delete the description of security requirement E2.91 in its entirety and replace with:

The Contractor must notify the GC by email and/or telephone (e-mail and telephone number to be determined) of any incident or potential incident, once detected, that could have an impact on GC data. The GC will determine the level of injury or potential injury and determine the course of action to be taken in conjunction with the Contractor.

CHANGE: 156

At *Annex 2 – Security and Privacy*, delete the description of security requirement E2.118 in its entirety and replace with:

From the date vulnerabilities are formally identified, the Contractor must expeditiously mitigate all vulnerabilities within a mutually agreed upon time frame between Canada and the Contractor.

(B) QUESTIONS**QUESTION: 491**

We respectfully ask the Crown to confirm that the closing date for this solicitation will continue to be extended as critical questions are asked and answered. After reviewing the recent amendments we will, along with our partners, be submitting questions we consider critical to responding to this RFP. In parallel, we are investing significant effort in writing a response and we ask the Crown to confirm that it will continue to extend the due date to a minimum of 6 weeks after all critical questions have been addressed.

ANSWER: 491

Canada extends the closing date of the RFP to 2:00 PM (EDT) on October 31st, 2016.

QUESTION: 492

Given this is a complex RFP that has undergone significant changes during the response period and which will require a large number of solution reviews and senior management approvals, we kindly request an extension of 10 days to the current due date. This will allow for the best possible response to the requirement.

ANSWER: 492

Canada extends the closing date of the RFP to 2:00 PM (EDT) on October 31st, 2016.

QUESTION: 493

Can you please provide an extension to October 17th 2016? We'll need additional time to address new and unanswered questions.

ANSWER: 493

Canada extends the closing date of the RFP to 2:00 PM (EDT) on October 31st, 2016.

QUESTION: 494

We respectfully request an extension to the closing date of the RFP. The changes that the Crown has made to the RFP in recent amendments are largely positive. The amendments have substantively improved the RFP and focused the requirements more clearly on the EPS as a SaaS Solution. At the same time, we note that the amendments have required bidders to revisit, re-price and re-approve their solutions. The current closing date of September 30 does not provide adequate time to properly solution, approve and write a response to these requirements. Given the likelihood that there are more changes and amendments yet to come, we believe it is reasonable to request an extension to October 21. This extension would provide time for Canada to respond to the final questions and for Bidders to absorb and respond to the requirements. Would Canada please extend the closing date by three weeks to October 21?

ANSWER: 494

Canada extends the closing date of the RFP to 2:00 PM (EDT) on October 31st, 2016.

QUESTION: 495

Based on the fact that there are still remaining questions to be answered we would ask that the Crown please extend the deadline to October 14th or 4 weeks after the last set of questions are answered.

ANSWER: 495

Canada extends the closing date of the RFP to 2:00 PM (EDT) on October 31st, 2016.

QUESTION: 496**3.3.2 Government Electronic Tendering Services (GETS)**

In order to supply financial estimates for Table 4 Tender Feeds, we will need to have more detailed requirements regarding third party tender feeds. Below are some key clarifications required:

- a) Are these third party tenders posted in the existing GETS portal today?
- b) In what file format will these tenders be provided? A PDF document, MS Word, email, etc.?
- c) Can/shall these third party tenders be reformatted or modified before being posted to GETS? Do these tenders need to be posted as is based on how it is provided by the third party or how it is posted on the third party sites?
- d) Who will be posting these tenders to GETS? By third party themselves or by PWGSC administrators? Will these tenders need to be reviewed by PWGSC before they are posted in GETS?
- e) What kind of integration and/or automation is required for the posting of these third party tenders to GETS?
- f) Will these tenders need to be physically stored in GETS/EPS or will it be sufficient for GETS to provide a URL link of the tender to the source system?

ANSWER: 496

For the benefit of Bidders, the optional defined work for third party tender feeds under section 7.2.4 *Tender Feeds* of the SOW are primarily intended to be leveraged to aggregate, publish and update tender notices from the Broader Public Sector (in particular provinces and territories) in support of the single point of access provisions of CETA as described in section 3.3.2.4 *Comprehensive Economic Trade Agreement (CETA)* of the SOW. The tender feeds may also be required to support feeds from other procurement systems within the GC during the transition period to EPS. For further clarity, a tender notice is not the tender itself, but rather the details of the tender necessary to provide a potential bidder the fundamental details of the opportunity. Bidders are encouraged to review Article 19.6.3 Notices of CETA for details of what a tender notice (referred to as a Notice of Intended Procurement in the CETA text) is required to contain.

In response to the specific questions raised by the Bidder:

- a) Third Party Tenders are not currently posted to GETS.
- b) A Canada-wide data standard for tender feeds has not been established. Canada anticipates establishing the tender feed standard in consultation with the Contractor and in discussion with the Provinces and Territories following Contract award and the entry into force of CETA. Canada further anticipates that the data format for tender feeds will be based on an open format such as XML or CSV.
- c) Yes, the format and presentation of the tender notice may be modified to conform with the standard format of the EPS GETS. The tender feed content itself however, must not be modified.
- d) A tender feed will be provided directly by the third party themselves (a particular province for example) and the tender notices contained in the feed are considered approved and ready for publication. As such, tender notices do not require additional workflow or approval prior to being posted.
- e) As consideration for the level of integration and automation required for the posting of tenders from third party sources is likely solution specific, Canada is not in a position to provide specific clarity on the architecture and approach. Suppliers are encouraged to review the requirements for tender notices in the RFP (including, but not limited to section 3.3.2.4 *Comprehensive Economic Trade Agreement (CETA)* of the SOW) to assess the manner in which tender feeds would need to be automated and integrated to meet the requirements in the context of the bidder's proposed solution.
- f) Bidders are reminded, as clarified above, that the tender notice is not the tender itself. For the purpose of the bidder's proposal, suppliers should assume that the tender notices will be required to be stored within EPS and that the tender notices will include a link to the tender itself in the source system.

QUESTION: 497**4.3 Interfaces with Government of Canada Systems**

Please share the version of Oracle ESB used at GC, and key modules and components used. Please clarify whether these modules include Oracle BPEL, SOA Suite and ODI, Oracle Data Integrator and Managed File Transfer licenses.

ANSWER: 497

To clarify, Canada expects the EPS to integrate with GCIP services that Canada will make available to the Contractor via the GCIP platform. The Contractor is not required to configure the GCIP or the GC back-end systems for interoperability. The GC will build and make available the GCIP services through an application gateway in order to interoperate with GC back-end systems. As stated in the answer to question #363, Canada will provision and be responsible for developing the necessary GCIP APIs and providing connectivity, i.e. GCIP platform and services, to GC back-end systems such as SAP DFMS. Should the GC require any additional GCIP services that need to be built by the Contractor, it will be raised via a Task Authorization.

GC currently has the following components in GCIP:

- Oracle Middleware Fusion 12c, with all default components
- SOA
- BAM
- BPM

QUESTION: 4984.3 Interfaces with Government of Canada Systems

For codes developed for ESB, should the bidder use GC's code version control and change/release management tools and processes? It is preferred and will provide GC better visibility and control of code deployed in ESB.

ANSWER: 498

The GC Interoperability group will be responsible for developing code in the GC ESB to expose internal GC systems to EPS. The Contractor will be required to provide SaaS integration code developed for EPS to GC and GC will leverage internal systems and processes for GC source code management and version control.

QUESTION: 499Annex 1, section 1.1

As stated in the RRR phase it would take a legal and business team several months to process this extensive list of Legislative, regulatory and policy requirements. Further these requirements change on a continual basis. In a SaaS environment it is unreasonable to expect the vendor to stay current on requirements and changes for public and private stakeholders across the globe. We request that this mandatory requirement be removed or changed to allow for "reasonable compliance".

ANSWER: 499

For clarity, the Contractor is not required to assess Canada's legislative, regulatory and policy requirements as part of the Transition-In nor is the Contractor required to continuously configure the EPS on an ongoing basis. As contemplated in 6.8.1.2 *Transition-In Delivery (or execution)* of the SoW, during Transition-In, Canada will articulate the business processes and rules required to comply with Canada's legislative, regulatory and policy requirements and the Contractor must ensure EPS is configured in a manner that ensures compliance with such legislative, regulatory and policy requirements.

As articulated in section 3.1 *Introduction to the Functional Requirements* of the SoW, the EPS must have the functionality to allow workflow and business rules to be configured by Users. Following Transition-In, Canada anticipates that it will manage additional required configurations to EPS to comply with changing legislative, regulatory and policy requirements. If the Contractor's support is required to perform these configurations, such work will be initiated on an as requested basis in accordance with section 7.2.1 *Additional System Configuration*.

QUESTION: 500Annex 1, section 4.3.2.4

This requirement appears to be for a non-SaaS EPS environment. Given that EPS will be a SaaS solution with well-defined integration points to existing systems using industry-standard protocols, would the Crown consider deleting this requirement? Alternatively, it is requested that the requirement be changed to "EPS must expose its functionality through an Application Programming Interface (API) that leverages industry-standard API protocols."

ANSWER: 500

As stated in section 4.3.2.4, the EPS must expose its functionality through an Application Programming Interface (API) that leverages industry-standard API protocols and Canada expects these APIs to be robust and fulsome to support GC's functional requirements as per the SOW in Annex 1. See the "Changes" section of this RFP amendment for a modification to section 4.3.2.4.

QUESTION: 501Annex 1, section A-01.01

We are unaware of any cloud vendor that complies with these standards in their entirety. These standards require features that are extremely expensive to implement and often would adversely affect performance of the system. Therefore implementing them in a multi-tenant environment is impractical. We believe we are compliant with the spirit of the standards. Therefore we request that this be moved to a rated requirement and evaluate the vendors based on their level of compliance.

ANSWER: 501

Section 5.8 *Web Accessibility* of the SoW outlines the level of compliance required and the manner in which Canada will assess compliance with the Standard on Web Accessibility requirement articulated in section A-01.01 of the SOW. For additional clarity, Canada will use the TBS assessment methodology checklist for WCAG2.0 compliance: <https://tbs-sct.gc.ca/ws-nw/wa-aw/wa-aw-assess-methd-eng.asp> which will assess if the Contractor has successfully implemented sufficient techniques and avoided common failures as listed in the checklist. If a success criteria fails to conform to WCAG 2.0 A or AA, the GC will assess the risks associated with the non-compliance.

In accordance with section 5.8 *Web Accessibility* of the SoW, operational activity of EPS may commence as long as the WCAG 2.0 compliance is substantially achieved with no critical deficiencies of the conformance requirements, such as a non-compliance resulting in a high risk of a failure to accommodate persons with disabilities (such as a visually impaired user unable to access the EPS). Canada has articulated a willingness, in accordance with section 5.8 *Web Accessibility* of the SoW, to assess and reasonably consider the Contractor's strategy and reasonable timeline to achieve compliance with the standard, which may include commitments to feature implementation in future releases.

Furthermore, Bidders should refer to the answer to question #508 and the "Changes" section of this RFP amendment where requirement A-01.01 is deleted.

QUESTION: 502Annex 1, section D-03.09

Can the Crown please provide an expected and reasonable estimate as to the number of supplier catalogues supported?

ANSWER: 502

The volumetric data that the GC has available is included in section 1.3 *Volumetric Data* in the Statement of Work. This data includes the number of Standing Offers and Supply Arrangements managed by PWGSC. The active Standing Offers and Supply Arrangements is available as Open Data here: <http://open.canada.ca/data/en/dataset/f5c8a5a0-354d-455a-99ab-8276aa38032e>

In addition to the Standing Offers and Supply Arrangement data, the GC does issue contracts with Task Authorizations that would also be included as a Catalogue. However, the data sets that we make available do not make a distinction between a contract with Task Authorizations and a contract without Task Authorizations.

QUESTION: 503

With respect to the one-page awareness training package referred to in section 6.4.2 Privacy Management Plan delivery where it states that "*The Contractor must provide within 60 business days of Contract Award a one-page awareness training package instructing the Contractor's resources regarding the use of the Personal Information provided by the GC about the Users*", we respectfully request clarification on the Crown's requirement. Although awareness and training are related, they are indeed different; will the expected deliverable be a 1-page employee privacy awareness briefing, or a more comprehensive training package?

ANSWER: 503

The expected deliverable is for a brief instruction document completed by the Contractor for the Contractor's employees on the use of Privacy and Personal Information. Please refer to section 7.5.2 *Privacy and Personal Information* of the Request for Proposal for additional information on how to apply the general clauses and conditions. Please see the "Changes" section of this RFP amendment clarifying the requirement.

QUESTION: 504

Regarding Q&A #454 provided in Amendment 21, the requirements such as those stated in Question 454 are generic and open to more than one solution, our proposed solution (as part of a standard SaaS offering) has existing capabilities to meet the stated requirements. Could the GC confirm which of the two scenarios will apply for the situation where the GC requests an alternative solution to the standard SaaS solution provided:

- a) The GC will adopt the standard SaaS solution as is; or
- b) The GC will use one or more Task Authorizations to request non-standard functionality and the solution for these generic requirements would be excluded from the Milestones' timelines, SLAs and Payments schedule.

ANSWER: 504

It is Canada's intention to adopt the winning Bidder's proposed EPS. It is the Bidder's responsibility to demonstrate its ability to meet the requirements of the RFP. Canada has endeavored to make the requirements generic to encourage competition in recognition that there may be more than one solution that meets the requirements. Should Canada have a need for additional functionalities beyond the requirements articulated in the RFP, Canada may leverage the Task Authorization process.

QUESTION: 505SOW Section 5.6 Service Desk

For service desk support, if a particular service ticket requires GC's attention, the ticket will be transferred to GC's support team. For instance, invoice processing error in DSMS. Can GC confirm that GC's support team would take ownership of the issue, and ensure its proper closure or resolution?

ANSWER: 505

Canada confirms that if an issue is related to GC systems and not related to the EPS, the GC will take ownership of the issue and manage the resolution.

QUESTION: 506Amendment #018, Q/A #389

GC has confirmed in this answer that "GC will be responsible for the training tools, such as a learning management system, and GC training processes." Can GC please further confirm that the training tools provided by GC include a knowledge base used for self-training of job aids, user guides, etc.?

ANSWER: 506

Currently, the GC learning management system does not have a knowledge base. It is anticipated that Canada will leverage a separate internal wiki for self-training of job aids, user guides, etc.

QUESTION: 507Amendment #009, Change #33

This change states that "Provide the training environment to reflect updates and upgrades to the production environment. The training environment must include all GC workflows and must interoperate with a GC managed DFMS training environment." Does this training environment have to be a dedicated training environment, can this environment be shared for development or testing activities?

ANSWER: 507

Please see the response to question #84 in Amendment #009. In accordance with 6.7.4. *Training Delivery* of the SOW, the Contractor must "provide the training environment to reflect updates and upgrades to the production environment and the training environment must include all GC workflows and must interoperate with a GC managed DFMS training environment". Given that development and testing environments, by their nature, contemplate new capabilities or configurations that are not yet reflected in the production environment, Canada will not permit the sharing of these environments with the training environment.

QUESTION: 508Annex 1 SOW Num A-01.01

Government of Canada's Web Standards established by the Treasury Board is quite extensive and works well with an on-premise or custom build web application. On the other hand, since a SaaS solution is a common solution used by many customers, including GC, it is not feasible to require a SaaS solution to comply all GC's web standard, of which some are unique only to GC. We kindly request GC to change this requirement to be a guideline only, and allow the SaaS vendor to make a good faith effort to adhere to this standard.

ANSWER: 508

Canada will delete requirement A-01.01 from Annex 1 – Statement of Work. Bidders are reminded of the clarified requirements for Web Accessibility articulated in section 5.8 *Web Accessibility* of Annex 1 – SOW and the privacy requirements in section 7.5.2 *Privacy and Personal Information* of the RFP.

QUESTION: 509Annex 1 SOW Num D-17.03

When a user logs in to EPS, it is expected that he or she is associated with a GC department/agency/client with respective cost center defined in a DFMS instance. Therefore, orders placed by this user should go into that DFMS and to that client for proper invoicing and account reconciliation. The requirement states that to split a Shopping Card when "i. Send Orders to the appropriate Client DFMS when there are multiple Clients associated to a Shopping Cart request". It is not supported by our SaaS solution. Can GC please provide a use case that a single shopping cart contains items that need to be processed for multiple clients? If this is not considered a critical requirement, we kindly request GC to remove this requirement or remove this particular example to avoid a high cost customization.

ANSWER: 509

Canada revised requirement D-17.03. Please see the "Changes" section of this RFP amendment.

QUESTION: 510Annex 1 SOW Num I-06.19

The requirement states that "for disposition classes to be systematically applied to existing, received or newly created records and associated Metadata, and where applicable group of records" For certain disposition classes mentioned in I-06.18, such as "destruction", systematic action is not appropriate and should not be allowed. We kindly request GC to change requirement to "for disposition classes to be systematically or manually applied to existing, received or newly created records and associated Metadata, and where applicable group of records".

ANSWER: 510

Please see the amendment to functional requirement I-06.19 in the "Changes" section of this RFP amendment.

QUESTION: 511

In its response to Question 258, Canada explained that it was not in a position to extend SSC's Procure to Pay Solution as GFE. Would Canada please confirm who owns the work and the intellectual property related to the SSC Procure to Pay Solution? At the same time, will the prime vendor of the SSC Procure to Pay solution have any ability to re-use the solution or the work provided to SSC in building its Response for EPS?

ANSWER: 511

SSC's Procure to Pay Solution was procured as an on premise managed service. Details of the procurement and resulting Contract for SSC's Procure to Pay Solution are available under the archived Solicitation #10030975/A on [buyandsell.gc.ca](https://buyandsell.gc.ca/procurement-data/tender-notice/PW-13-00357466) (<https://buyandsell.gc.ca/procurement-data/tender-notice/PW-13-00357466>).

While nothing prevents the prime vendor of the SSC Procure to Pay solution from leveraging their experience in their response and the delivery of EPS, it should be noted that the context and scope of the two solutions are different and Canada is not in a position to confirm or assess the extent that the work can be re-used in the delivery of EPS.

QUESTION: 512Annex 2, section E2.15

Please confirm that (a) this question is related to restrictions for operators, or cloud administrators, and not end users. It is unreasonable to expect a SaaS solution to control any hardware-specific feature or function on a desktop.

Please confirm (b) that the requirement is simply to restrict portable media from the point of storage, which is at the data center.

ANSWER: 512

- (a) Canada confirms that restrictions are related to operators, or cloud administrators, and not end users.
(b) Please refer to the response to question #428 in Amendment #020.

QUESTION: 513Annex 2, section E2.21

In a SaaS environment vendors provide standard log events. In c) given that the Crown has not specifically identified log events to be approved, we request that this requirement further be defined. For example the following is provided in a SaaS environment:

- 1) Application log, which logs events related to your solution and your data, including login, logoff and most transaction activity.
- 2) Also log events that are related to the network, such as operation system, database, and IDS/IPS traffic.

As part of the service, we would monitor and manage security events (according to ISO 27035).

The Crown will have immediate access to the application log, but would not be provided access to the network logs. Additionally, logged events are predetermined, include most if not all transaction and logon/off activity.

ANSWER: 513

During the SA&A process, Canada will review the proposed EPS standard log events for conformance to the security requirement. All gaps will be identified as part of the EPS SA&A gates review and will be shared with the Contractor for remediation. Canada expects that GC EPS Application and associated infrastructure logs containing GC EPS Data will be available to Canada throughout the Term of the Contract or sufficient material to permit Canada to identify and assess the issues.

QUESTION: 514Annex 2, section E2.23

As part of the SaaS service, storage is managed. Capacity is generally managed to 70% utilization, and we maintain excess capacity on demand. Should additional resources be required, we would add additional capacity.

Given that this is the SaaS vendors responsibility, and that it is the vendor's responsibility to provide and manage appropriate capacity, we request that the Crown remove any requirements for alerts back to Crown in this regard?

ANSWER: 514

For clarity, requirement E2.23 (c) will be modified to state the "Contractor's Operations Centre" instead of "Operations Center".

QUESTION: 515Annex 2, section E2.28

In a SaaS environment the host organization is responsible for availability per the SLA's. How this is delivered is the responsibility of the vendor. In a multi-tenant SaaS Environment, there would be little advantage to maintaining multiple baselines (current + 2 previous version).

We request that the Crown retract the requirement to maintain previous versions and maintain the baseline version only?

ANSWER: 515

For clarity, the requirement for configuration management relates to the EPS configuration and not to the SaaS application and is intended to allow Canada to revert to previous configurations of EPS in the event that a new configuration creates issues that cannot be remedied.

During the SA&A process, Canada will review and assess the proposed EPS configuration management plan to determine if the plan is adequate. See the "Changes" section of this RFP amendment for a modification to this requirement.

QUESTION: 516Annex 2, section E2.60

This requirement applies to a managed hosted solution. We request that SaaS providers be required to list the third party audit standards that map to this requirement.

ANSWER: 516

During the SA&A process, Canada will assess the mapping and all related evidence to verify and validate for conformance as it is stated within the RFP.

QUESTION: 517Annex 2, section E2.85

Please provide specific criteria for a), b), c) and d) such that vendors can respond to the requirement. Alternatively we request that the Crown use International standards (example ISO27001, ISO22301) as the baseline for measurement.

ANSWER: 517

The requirement E2.85 relates to the incident response capability as provisioned within the Contractor's EPS. The specific criteria for items detailed under (a) to (d) will be dependent on the type and nature of the security incident. During the SA&A process, Canada expects that the Contractor will provide evidence details, including leveraging 'like for like' international standards, as applicable for this requirement, for Canada's assessment of conformance. Requirement E2.85 in Annex 2 will be amended for clarity.

QUESTION: 518Annex 2, section E2.91

Please provide specific priority such that vendors can respond to the requirement.

ANSWER: 518

The purpose of requirement E2.91 is to make sure that Canada is informed in time of all the security incidents related to the EPS and associated data. Furthermore, Canada considers all security incidents associated with the EPS and its data as a priority and hence expects to be notified per the details specified within the requirement. Please see the "Changes" section of this RFP amendment for clarification to requirement E2.91.

QUESTION: 519Annex 2, section E2.93

It is impossible for vendors to agree to a non-exhaustive list. ("but is not limited to")

In a SaaS environment vendors adhere to ISO security standards. Vendors should be required to align with reporting as outlined in international standards. Can the Crown please confirm that this will be acceptable?

ANSWER: 519

During the SA&A process, Canada will assess the capability offered with respect to the requirement detailed under E2.93. The Contractor can leverage 'like for like' third party standards to demonstrate conformance to the specific elements listed from (a) to (o). Any gaps based on the SA&A process with respect to requirement E2.93 will be internally reviewed by Canada for decision on necessary remediation by the Contractor or for risk acceptance.

QUESTION: 520Annex 2, section E2.118

Vulnerabilities may occur in any number of areas including but not limited to operating system, database and or other hardware, firmware and software. The vendor would need to rely on the manufacturer to make a patch available. Therefore it is unreasonable for the Crown to expect remediation according to the timelines described.

Will the Crown amend the requirement and accept that vulnerabilities be resolved based on the priority, classification and impact to the system?

ANSWER: 520

Canada will amend requirement E2.118 to provide clarity. Please see the "Changes" section of this RFP amendment.

QUESTION: 521Annex 2, section E2.124

Multi-tenant SaaS vendors are aligned to internationally recognized standards. Will the Crown accept an international standard that could be mapped to these ITSG standards?

ANSWER: 521

Canada will accept evidence based on an international standard that clearly demonstrates a 'like for like' comparison with the security requirements of *Annex 2 - Security and Privacy*.

QUESTION: 522

While we are mindful of the requirement to segregate GC EPS data from that of other customers, in a SaaS context, shared elements such as log collection, security and network monitoring would normally be managed and monitored using existing shared consoles and SIEM systems, with GC-specific forensic investigative data to be stored on approved storage. Please confirm this understanding is consistent with the Security Requirements identified in both Annex 1 Rev 2 of the SOW, as well as the security controls assigned for EPS, including (but not limited to) E2.11, E2.80, and E2.141.

ANSWER: 522

Canada understands that the SaaS model being proposed for EPS will influence the level and extent of separation for the GC Data. The use of shared resources, such as consoles and SIEM systems and GC-specific forensic investigative data residing on approved storage, must at all times comply with confidentiality, integrity and availability requirements as stated within *Annex 2 - Security and Privacy* as well as the associated SRCL throughout the Term of the Contract.

QUESTION: 523SOW Section 6.5.1 IT Security Operations Center

As some of the security incidents may involve GC applications that are not part of EPS, does GC have a dedicated SOC that EPS support team can work with for incident reporting and resolution in this case?

ANSWER: 523

The GC will identify the dedicated point of contact for the Contractor to work with for incident reporting and resolution following Contract award.

QUESTION: 524SOW Section 6.5.1 IT Security Operations Center

Does the SOC number need to be a separate number, or is it acceptable to use one common number that addresses all incidents, including security incidents?

ANSWER: 524

Please refer to the response to question #418 in Amendment #019.

QUESTION: 525**Annex 2 SECTION III - SERVICE LEVEL AGREEMENTS**

The requirement states that "The Contractor should employ an independent assessor or assessment team to conduct an assessment of the security controls in the information system." Can GC please confirm that the "assessment team" can come from an independent business unit within the bidder's or team member's organization?

ANSWER: 525

Canada confirms that an independent assessor or assessment team from an independent business unit within the Bidder's or team member's organization with no conflicts of interest and able to perform an objective, impartial, and independent assessment of the security controls in the information system using competent resources will be acceptable.

QUESTION: 526**Annex 2 Security and Privacy E2.12**

As we understand that Annex 2 is considered a guideline, we would still like to get further clarifications from GC on certain security and privacy requirements. This requirement E2.12 states that "The Contractor must establish Policies and procedures, supporting business processes and technical measures, implemented within any environments supporting the EPS in order to protect EPS from wireless network environments". For a SaaS based solution, the application can be accessed outside of GC's intranet, therefore, local wireless/wifi control is not applicable. Can GC confirm that this requirement is not relevant to EPS?

ANSWER: 526

Canada clarifies that the scope of 'wireless network environments' as stated within requirement E2.12 is limited to the Contractor's EPS facilities and supporting infrastructure and does not include end users and the GC's Intranet.

QUESTION: 527**Annex 2 Security and Privacy E2.29**

This requirement E2.29 states that "The Contractor must only allow authorized software, as documented by the Contractor and approved by Canada, to execute on the EPS." For a SaaS based solution, the software installed on SaaS is tightly controlled and managed by the SaaS provider. On the other hand, the installation of these software is solely at the discretion of their SaaS provider, therefore, approval from GC does not apply here. Can GC confirm that this requirement is not relevant to EPS, or provide further clarifications?

ANSWER: 527

Canada expects that during the SA&A process, the Contractor will provide the specific evidence related to this requirement for conformance review and assessment. The Contractor must maintain and use the processes and mechanisms as described and accepted through the SA&A process and throughout the Term of the Contract. As such, requirement E2.29 will be amended.

QUESTION: 528**Annex 2 – E2.12 – "User access including operators..."**

While we can control access to our cloud infrastructure, it is not reasonable to expect we can control your wireless access points (WAPs) or access through your wireless points or devices. We recognize this is a subtle distinction, but we request this simple point of clarity to reflect that this requirement would only be for administrative operators and not for end users. End user management, including wireless access would be the responsibility of the crown. Additionally, consider that any solution that is accessed through a web browser could also be accessed by a mobile device (phone, tablet, or laptop).

Will the Crown also clarify this is referring to WAPs on the contractor site?

ANSWER: 528

Yes, Canada confirms that this refers to WAPs on the Contractor's site(s). Please refer to the answer to question #239 in Amendment #013.

QUESTION: 529

Annex 2 – E2.13 – “The Contractor must implement a mobile device policy...”

In Amendment 13, question 239, it was asked whether Mobile Device Management (MDM) was to be included, but the response was that the policy was required. We understand MDM is not in scope for the solution. We have the following questions/clarifications:

- a) Can the Crown clarify if this requirement is related to MDM for the solution or in support of the EPS solution within the contractor environment?
- b) Will the Crown please also confirm that this requirement relates to the contractors use of MDM for mobile devices connecting to EPS. For example in the administration of EPS?

ANSWER: 529

a) Canada confirms that the requirement related to Mobile Device Management (MDM) is in support of the EPS within the Contractor's environment.

b) Canada confirms that in regards to the MDM, Canada expects the scope of this capability in the context of the RFP to be limited to Contractor resources supporting the EPS.

QUESTION: 530

Annex 2 – E2.40 - “The Contractor must provide GC with the EPS operational security procedures that include operational roles and responsibilities for contingency planning.”

As part of the solution, Business Continuity and Disaster Recovery services are included in the service. However, it is limited in scope to our solutions provided. Customers typically address their internal BC/DR plans themselves, to address the additional scope of recovering their internal systems and incorporating our cloud continuity. We have the following questions/clarifications:

1. Will the Crown please confirm it will accept the contractor's responsibility as limited in scope to the services we provide, while PSPC would ultimately develop a full plan to include the contractors BC/DR and the Crown's internal systems?
2. Will the Crown allow the Contractor to limit BC/DR planning for the scope of responsibility – for the services to be provided?

ANSWER: 530

In accordance with evaluation criterion *R4.4 IT Service Continuity Plan* of the Technical Evaluation, Canada confirms that the Contractor's scope regarding business continuity and disaster recovery is the EPS services provided by the Contractor. Canada will include the Contractor's IT Service Continuity Plan as a component of its operational business continuity plans.

QUESTION: 531

RFP section 2.1.3

SACC 2003 - Standard Instructions - Goods or Services - Competitive Requirements, including the Ineligibility and Suspension Policy and the Code of Conduct for procurement.

14 (2007-11-30) Price justification

In the event that the Bidder's bid is the sole responsive bid received, the Bidder must provide, on Canada's request, one or more of the following price justification:

- a. a current published price list indicating the percentage discount available to Canada; or*
- b. a copy of paid invoices for the like quality and quantity of the goods, services or both sold to other customers; or*
- c. a price breakdown showing the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, etc., and profit; or*
- d. price or rate certifications; or*
- e. any other supporting documentation as requested by Canada.*

We cannot accept this clause as-is. We suggest the following change. Deletions are ~~stricken through~~ and additions are underlined.

14 (2007-11-30) Price justification

In the event that the Bidder's bid is the sole responsive bid received, the Bidder must provide, on Canada's request and if available, one or more of the following price justification:

- a. ~~a current published price list indicating the percentage discount available to Canada; or~~*
- b. an anonymized copy of paid invoices for the like quality and quantity of the goods, services or both sold to other customers in Canada; or*
- c. ~~a price breakdown showing the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, etc., and profit; or~~*
- d. price or rate certifications; or*
- e. ~~any other supporting documentation as requested by Canada.~~*

ANSWER: 531

In the event that only one Bidder is responsive, Canada must be able to verify that it is obtaining best value in the award of the Contract. The elements listed in the *Price justification* section of SACC 2003 will assist Canada with this verification. As such, this section will remain unchanged.

QUESTION: 532Section 4.2.1.1

Bid Evaluation for SCSI states that bidder will have 2 working days to provide the necessary information to Canada if Canada requires any additional information. We request that this be increased to 5 working days due to the nature of the information?

ANSWER: 532

As detailed in section 4.2.1.1 of the RFP, "(t)he Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada". Canada will reasonably consider the nature of the information when deciding whether to provide or not a longer period to the Bidder. As such, this section will remain unchanged.

QUESTION: 533RFP section 7.18

The standard clause is not acceptable in a SaaS environment in its current state. It creates a situation where, for SaaS Services, the cap on liability is ever growing. Considering the duration and nature of this opportunity, the exposure to the SaaS vendor is exponential.

We can accept this clause as-is for Professional Services however, for SaaS Services, we respectfully request that the Cap on Liability under paragraph (e) be limited to the value of the SaaS Services provided in the twelve months preceding the event that gave rise to the claim.

ANSWER: 533

The cap on liability under paragraph (e) was already reduced through a revision, in Amendment #021, to "0.25 times the total estimated cost (...) or \$1,000,000.00" to align with Canada's pre-approved liability limits for the Commercial Software and Maintenance IM/IT commodity grouping and takes into account a balanced management of risk by Canada. As such, this clause will remain unchanged.

QUESTION: 534RFP section 7.25

In case of unauthorized access to Canada's data, Canada expects to be notified as soon as possible but no later than 24 hours after the Contractor became aware of the breach. The Contractor does not commit to a timeline. Can the Crown remove the 24 hours requirement and leave it to as soon as possible?

ANSWER: 534

The integrity of Canada's data in EPS is essential to the integrity of Canada's procurement process. Compromises to Canada's data are considered of very high significance and priority, with time of the essence as delays may cause material harm to Canada and its stakeholders. Therefore, such events must be communicated to Canada within 24 hours of becoming aware of such occurrence. As such, this clause will remain unchanged.

QUESTION: 535

RFP section 7.27

We would request that the following be added to this section:

Considering the lengthy process that lead to this proposal, as well as the significant amount of changes that took place during the process, Canada acknowledges that many iterations and amendments were made during the RFP process, and that the statements and representations made by the Contractor must be assessed in light of the relevant amendments and changes made to the RFP.

ANSWER: 535

Clause 7.27 *Representations and Warranties* of the RFP pertains to the information contained in a Bidder's bid. Given that, by submitting a bid, the Bidders must take into account the RFP and all of its amendments, Canada will not include this statement in this clause. As such, the clause will remain unchanged.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.