



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. 014
Client Reference No. - N° de référence du client 20131350	Date 2016-07-12
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 2016-08-10	
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: 014****Purpose:**

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

(A) CHANGES**CHANGE: 86**

At *Attachment 2 to Part 4 - Technical Evaluation*, in column "Bid Submission Requirements" of evaluation criteria *R4.1* of section *4. Point-Rated Criteria*, delete bullets *ii.* and *iii.* in their entirety and replace with:

ii. a description of how the deployed model can meet the current scalability needs (based on existing Government of Canada volumes as outlined in *section 1.3 Volumetric Data of Annex 1 - SOW*), future scalability needs (based on the expansion to the Broader Public Sector), and performance Service Level Agreements (SLAs) described in this solicitation including through peak periods in business cycles.

The description should include, but is not limited to:

a) established practices, tools and processes to monitor, track and to manage scalability and performance issues;
b) architectural models, features and design that support the proposed solution scalability and performance; and
c) examples of expected and unexpected scalability and performance demands and their resolution, based on real-life experiences of Bidder's customer(s) who are of similar size and scope as the EPS.

iii. an EPS data management plan that identifies EPS data, meta-data, their format, defaults and describes policies and strategies on data security, access, sharing, storage, and disposition, etc. The Bidder should include a master data plan that describes the solution's master data set, strategies, processes and pre-requisites to interoperate with GC's back-office systems.

CHANGE: 87

At Annex 1, section *6.8.1.3 Transition Integration and System Testing*, delete *d)* in its entirety and replace with:

d) Conduct all system testing in accordance with the approved testing strategy and plan; and

CHANGE: 88

At Annex 5 - Glossary, add the following:

Mobile Code: A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.

CHANGE: 89

At *Annex 2 – Security and Privacy*, delete the description of security requirement E2.113 in its entirety and replace with:

The Contractor must implement at alternate work sites management, operational, and technical security controls that achieve the same objectives as those implemented at the main PWGSC EPS Facility. Alternate site(s) must be approved concurrently with the Primary sites by CISD/IISD.

CHANGE: 90

At *Attachment 2 to Part 4 - Technical Evaluation*, in column "Bid Submission Requirements" of evaluation criteria *R5.6* of section 4. *Point-Rated Criteria*, delete bullets *i.* and *iii.* in their entirety and replace with:

i. The strategy for continuous monitoring;

and

iii. Details of data collection and its reporting aspects;

CHANGE: 91

Delete section 7.3 *EPS Warranty and Maintenance* of the RFP in its entirety and replace with:

7.23 EPS Warranty and Maintenance**7.23.1 EPS Warranty:**

The Contractor warrants and represents that the EPS will meet or exceed all of the requirements set out in the Contract during the entire Term of the Contract.

7.23.2 EPS Maintenance:

a. The Contractor must ensure that, as a minimum, the EPS works with Microsoft Internet Explorer 11, including compatibility mode; and

b. The Contractor must ensure that the EPS works with all future commercially available versions of Microsoft Internet Explorer (version 11) and 2 previous versions (version 11 - 2). This requirement is in effect as of Microsoft Internet Explorer 11.

(B) QUESTIONS**QUESTION: 289**

Given the uncertainty of the volume of spend to be managed through the Bidder's solution, as well as the Software as a Service (SaaS) approach, we suggest the Government of Canada include in the RFP an assessment of the Bidders' proposed SaaS infrastructure proven ability to scale to support an undefined volume. The related requirement R4.1 ii) does not indicate the extent of the required scalability and we suggest this lack of clarity increases the risk to the Government of Canada. We therefore recommend the following addition to R4.1 "The Bidder should describe how the proposed solution's SaaS infrastructure is currently used to support procurement volumes in excess of \$19B annually."

ANSWER: 289

Attachment 2 to Part 4, R4.1 has been amended. Please see the "Changes" section of this RFP amendment.

QUESTION: 290

We have identified a number of items for clarification that would improve the Bidder's ability to estimate the EPS. Would Canada please clarify the following estimating factors, based on current volumes:

- a) Number of contracts which are estimated to be created in EPS annually or monthly
- b) Number of sourcing projects which will be raised via EPS annually or monthly
- c) Number of Purchase orders which will be raised via EPS annually or monthly
- d) Number of Invoices which will be raised via EPS annually or monthly
- e) Are there any purchased items that are inventory managed? Is that managed in DFMS or another system?
- f) What data is posted in OpenData? What data fields? What business service is supported? How many users access that data?
- g) How many Procurement portals are currently used, Internal and/or external?

ANSWER: 290

- a) Please see Annex 1 Statement of Work, Section 1.3 Volumetric Data for data regarding the historical number of contracts.
- b) Please see Annex 1 Statement of Work, Section 1.3 Volumetric Data for data regarding the historical number of sourcing projects.
- c) Please see Annex 1 Statement of Work, Section 1.3 Volumetric Data for data regarding the historical number of Purchase orders under the Title Call-ups. Please note the information for the number of Task Authorizations that are issued under a Contract with Task Authorizations is not available.
- d) The GC cannot predict the number of invoices that will be raised via EPS. Unfortunately, the GC is unable to breakdown the historical information to provide the number of invoices that the GC currently process just related to Contracting and Procurement.
- e) Yes purchased items that are inventory managed are managed within the DFMS. EPS will contain no inventory management information.
- f) Details regarding the data dictionaries for Open Data are detailed on the website for the given data set. For reference, the applicable open procurement data sets are detailed below. For clarity, the EPS is not required to host open data sets but must, in accordance with 1.2.7 Open Data, aggregate and provide open procurement data sets for the purposes of publishing by the GC.

Tender Notices:

<http://open.canada.ca/data/en/dataset/ffd38960-1853-4c19-ba26-e50bea2cb2d5>
https://buyandsell.gc.ca/cds/public/datadictionary/tpsgc-pwgsc_dd.xml (includes field's definition)

United Nations Standard Products and Services Code

<http://open.canada.ca/data/en/dataset/92214e02-bb86-433e-81b9-c2a78a518e75>

https://buyandsell.gc.ca/cds/public/datadictionary/tpsgc-pwgsc_dd.xml (includes field's definition)

Contract History

<http://open.canada.ca/data/en/dataset/53753f06-8b28-42d7-89f7-04cd014323b0>

https://buyandsell.gc.ca/cds/public/datadictionary/tpsgc-pwgsc_dd.xml (includes field's definition)

Standing Offers and Supply Arrangements <http://open.canada.ca/data/en/dataset/f5c8a5a0-354d-455a-99ab-8276aa38032e> https://buyandsell.gc.ca/cds/public/datadictionary/tpsgc-pwgsc_dd.xml (includes field's definition)

Goods and Services Identification Number <http://open.canada.ca/data/en/dataset/2ce347e5-02fd-4487-975d-67a435efdf9b> https://buyandsell.gc.ca/cds/public/datadictionary/tpsgc-pwgsc_dd.xml (includes field's definition)

Government of Canada Spend Data by Department <http://open.canada.ca/data/en/dataset/c37d7510-c54c-4652-8e6f-79023e44be62> https://buyandsell.gc.ca/cds/public/spends/tpsgc-pwgsc_depenses-spend_dd.xml (includes field's definition)

Government of Canada Spend Data <http://open.canada.ca/data/en/dataset/078af0f7-4b15-455d-a466-db5c44409205> https://buyandsell.gc.ca/cds/public/spends/tpsgc-pwgsc_depenses-spend_dd.xml (includes field's definition)

g) Existing procurement portals (such as *BuyandSell.gc.ca*) are the responsibility of the GC. The Contractor will not be responsible to manage or interface to any of the existing procurement portals.

QUESTION: 291

Attachment 1 to Part 4, Evaluation and Selection Methodology, Proof of Proposal Test.

The proof of proposal (POP) test states that the Bidder will be given a maximum number of 5 working days to prepare. To provide a better presentation and accommodate resource management across multiple clients and geographies, it is requested that the Crown provide 15 working days for preparation.

ANSWER: 291

Please refer to the answer to question #108.

QUESTION: 292

Regarding Annex 1, Section 6.8.1.3, please confirm that load testing is not required if a Bidder is proposing a multi-tenant cloud solution and infrastructure with a proven ability to support loads exponentially larger than those of required by the Crown.

ANSWER: 292

In accordance with section 6.8.1.3, the Contractor must propose a testing strategy and plan and must recommend testing requirements to verify that the solution meets the functional, performance, and reliability requirements of the SoW. Canada's acceptance of the proposed testing strategy, which may contemplate various techniques or mechanisms to demonstrate the solution's performance under load, will be based on the adequacy of the proposed strategy to verify that the requirements are met. For clarity, should the proposed testing strategy be inadequate, Canada may require load testing from the Contractor. Please see the "Changes" section of this RFP amendment providing clarity that the system testing must be in accordance with the approved testing strategy and plan rather than performance of defined types of system testing.

QUESTION: 293

Section 7.1 (page 26)

The ownership of suppliers' private information including the content of their responses in response to any requirement is proprietary to each supplier. Could the crown confirm that all suppliers to the government have released consent that their information could be stored in third-party databases, whether or not these third-parties could have or be perceived to have business ties with these government suppliers' competitors within and outside Canada. We understand that the crown is taking a business risk by privatizing its procurement body in this venture by storing data outside the crown's architecture as this architecture will not be owned nor maintained by the crown. Could the crown confirm that as a contractor, our firm and our partners will not be considered in a perceived conflict of interest as a result of being awarded the contract under this RFP and that this contract award will not prevent our firm nor our partners and subcontractors to bid on future government contracts regardless of the commodity being acquired through the use of our solution?

ANSWER: 293

In accordance with Section 7.5.2 d) Collection of Personal Information, if the Contractor must collect Personal Information from a third party to perform the Work, the Contractor must only collect Personal Information that is required to perform the Work. The Contractor must collect the Personal Information from the individual to whom it relates.

The Contractor must inform that individual at or before the time it collects the Personal Information, of the following: (i) that the Personal Information is being collected on behalf of, and will be provided to, Canada; (ii) the ways the Personal Information will be used; (iii) that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement; (iv) the consequences, if any, of refusing to provide the information; (v) that the individual has a right to access and correct his or her own Personal Information; and (vi) that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the Contractor.

If requested by the Contracting Authority, the Contractor must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone.

Canada confirms that being awarded a Contract under this RFP will not prevent the Contractor from bidding on future government contracts. However, in accordance with section 18 of SACC 2003 Conflict of interest—unfair advantage, Canada may reject a bid from a Bidder if, in Canada's opinion, they had access to information that would give or appear to give the Bidder an unfair advantage. Canada reserves the right to exercise the full extent of the law and remedies under the Contract should a matter concerning inappropriate or unlawful access to competitive information arise.

The Contractor is responsible for ensuring that their conduct and performance of the Work does not result in criminal activity (e.g. unfair competitive advantage) or place themselves in a real or apparent conflict of interest.

QUESTION: 294

Please confirm that the crown is assuming all costs that could occur as a result to be awarded the contract by the contractor that are associated with government suppliers challenging the successful contractor for perceived loss of revenue or perceived loss or access to intellectual proprietary and business information as a result of their information residing within the contractor's infrastructure? This is important as the crown will not own the solution but acquiring an access license and that the resulting contract includes a clause allowing the crown to terminate the contract for convenience at any time.

ANSWER: 294

Canada does not confirm. Liability for damages resulting from performance of the Work will be treated in accordance with the law and the Terms and Conditions of the Contract.

QUESTION: 295

Section 7.4.1 c. (i) and Section 7.4.2

Could the crown confirm that no rights on any bi-products created as a result of third-party suppliers' data residing on the winning vendor's architecture such as acquisition trend analysis, statistics, patterns, etc. applied to some or all data, whether it is government data or suppliers' data, whether it is done at the crown request or not, are being provided to the winning vendors nor in the hand of any of its employees or partners. Under 4006 – Contractor to own intellectual property right in foreground information, many bi-products may end to fall under the intellectual property of the contractor to the detriment of suppliers. As technology is evolving at fast pace, and the possibility is endless in relation to data, it seems that the crown is making mandatory that suppliers to the government to bear the business risk to allow the crown to store their data outside the government infrastructure within a third-party if they want to continue doing business with the government. Please confirm that it is the crown's intent to diminish the number of suppliers to the government.

ANSWER: 295

In accordance with section 7.2 *Supply Chain Security Information (SCSI) Assessment Definitions* and 7.24 *Contractor Use of Canada's Data* of the RFP, Canada owns all data originating from the Work, any data received in contribution to the Work or that is generated as a result of the delivery of security, configuration, operations, administration and management services, and any data that is transported or stored by the Contractor or any subcontractor as a result of performing the Work. The Contractor is provided a limited license, for the Term of the Contract, to Canada's Data for the sole and exclusive purpose of performing the Work, including a license to collect, process, store, generate, and display Canada's Data only to the extent necessary in the provision of the Work. The Contractor must not use, sell, rent, transfer, distribute, or otherwise disclose or make available Canada's Data for the Contractor's own purposes or for the benefit of anyone other than Canada without Canada's prior written consent.

Canada does not confirm that it is Canada's intent to diminish the number of suppliers to the government.

QUESTION: 296**Section - 7.5 Security Requirements**

Understanding that it is foreseen that there may be a crown's business decision at a future date to request suppliers' confidential information that is the "bread and butter" of any Canadian and Foreign suppliers to reside outside the government of Canada's architecture and understanding the malicious IT attack done on an ongoing basis against any IT technical environment as evidenced by the release to the world of private citizens bank information recently on the news that were stored in very high security IT environment, we are concerned about the low level of security associated with this requirement for approved document safeguarding which is only at protected B with personnel at the reliability status level. We are concerned that the crown may award the contract to a vendor who have not make the same high level of investment toward security.

ANSWER: 296

Canada has completed significant engagement with both industry and its security agencies and is of the opinion that the security requirements contained in this RFP are appropriate.

Canada will not store data above the level of Protected B in the solution.

As well, several safeguards are built into the requirement including the requirements of *Annex 2 – Privacy and Security*, evaluating IT security as part of the evaluation process and the SCSI assessment.

QUESTION: 297

There was a recent public announcement on May 24, 2016, by PWGSC Minister to announce a \$322 million contract to update SSC's enterprise data center in Borden. Could the crown provide the rationale behind the business decision from Shared Services Canada to not allow a solution that dealt with third party proprietary data to store data within the government environment to ensure that suppliers' data are secured in an environment that is maintained within government infrastructure? Please confirm that the highest instances of the federal government have provided their consents as tremendous level of efforts are being deployed by our partners at this moment.

ANSWER: 297

PWGSC consulted with all necessary government departments, including Shared Services Canada, as well as industry in the development of its requirement. Canada also obtained all necessary approvals from senior government officials related to the release of this RFP.

QUESTION: 298

The privacy act is about "personal information" of individual and about the information residing within government's infrastructure. As the data will not reside on government infrastructure and a large portion of the data will be about third-party information (suppliers), could the crown provide information on how this privacy act is relevant in this context (data is residing outside GC)?

ANSWER: 298

For clarity, the Privacy Act is with respect to personal information about individuals held by a government institution. Residency of data or information is not a consideration of the Privacy Act. The fact that Canada has possession of records, for example, whether in a legal or corporeal sense, is sufficient for such records to be considered "under the control" of the government institution and subject to the Access to Information Act and the Privacy Act.

Under the Contract, Canada maintains both the legal right and the contractual obligation to retrieve the information, data, and documents from third parties upon demand. Thus, this information is under the control of Canada and is subject to the Access to Information Act and the Privacy Act

In accordance with Section 7.2 Supply Chain Security Information (SCSI) Assessment Definitions and 7.24 Contractor Use of Canada's Data of the RFP, Canada owns all data originating from the Work, any data received in contribution to the Work or that is generated as a result of the delivery of security, configuration, operations, administration and management services, and any data that is transported or stored by the contractor or any subcontractor as a result of performing the Work. The Contractor is provided a limited license, for the Term of the Contract, to Canada's Data for the sole and exclusive purpose of performing the Work, including a license to collect, process, store, generate, and display Canada's Data only to the extent necessary in the provision of the Work.

QUESTION: 299

Section 7.5.2

The definition of "personal information" is about individual and that definition seems to apply to the content of the privacy act. We have found instructions into the Supply Manual published on the government buyandsell website that states: "PWGSC must ensure that safeguards are put in place to protect individual and company private information by ensuring information is stored securely and that information is handled through limited distribution and provided only as necessary. Under no circumstance should a company's private information or an individual's personal information be shared with competitors or placed in the public domain without the written authorization of the originator of the information." We are concerned that this statement may prevent our firm, our partners and all our subcontractors to bid on future government contracts. Could the crown confirm that this will not be the case and there will be no restriction that apply to the winning vendor although as part of the Work, the winning vendor will create, collect, receive, manage, access, use, retain, disclose and dispose of personal information that may belong to a competitor.

ANSWER: 299

Please refer to the answer to question #293.

QUESTION: 300

Section 7.5.2 (d) (iv)

The RFP states that it is the winning vendor (contractor and its subcontractors and employees) and not government employees that will seek the personal information directly from suppliers as the winning vendor must identify itself to the Canadian and foreign suppliers of the government. We understand that the consequences of refusing to provide information to the winning vendor will lead to existing or future potential suppliers to the Canadian government to being unable to obtain future contracts with the crown. We are concerned that these suppliers to the Canadian government may potentially raise legal complaints against our firm if we are the winning vendor and that the risk if it materialized could be costly to our firm and to our partners. Could the crown confirm that the winning vendor will be fully compensated by the crown against such risks?

ANSWER: 300

Canada does not confirm. Liability for damages resulting from performance of the Work will be treated in accordance with the law and the terms and conditions of the Contract.

QUESTION: 301

Section 7.5.2 (d) (page 38)

RFP states: "... if the Contractor doubt that the individual has the capacity to provide consent to the disclosure ..."

Could the crown provide scenario where doubt could be based? What will be the legal ramification and business risk to the winning vendor in a situation where consent is received and process from an individual that does not have the capacity? Will the crown impose some requirement to the winning vendor? If yes, what will it be as this will impact the financial response.

ANSWER: 301

As the collection of personal information is expected to be exclusively through electronic means, it is unlikely that a scenario will arise where the Contractor will be in a position to reasonably assess the capacity to consent of the individual providing the information. However, should employees of the Contractor that come into contact with individuals (such as call center personnel) require the collection of personal information in the performance of the Work, then this scenario may arise.

The ability for an individual to consent is a matter of law and Bidders are advised to seek legal guidance on clarity as Canada is not in a position to provide Bidders with legal advice or advice on the assessment of risk in the delivery of the Contract.

QUESTION: 302

Section 7.5.2 e) (page 38)

We are concerned that this section referenced only individual's private information and does not address suppliers' private information. Could the crown amend this section to address the omitted text.

ANSWER: 302

For the purpose of the Privacy Act, a corporation is not considered an individual and business confidential information provided by a supplier would not constitute personal information. However, information related to a sole-proprietorship or a partnership could constitute personal information if it constitutes information about an identifiable individual. Additionally, Professional or work-related information about an individual may be classified as personal information.

QUESTION: 303

Section 7.5.2 (f) – page 39 – under safeguarding personal information

It states: "Canada reserves the right to request implementation of additional reasonable measures and solutions from time to time."

As we are unable to foresee what these measures and solutions will be nor the timeframe for such request, could the crown confirm that the crown will pay entirely for the implementation of these measures and solutions being requested from time to time. Could the crown provide a definition of "reasonable measure"?

ANSWER: 303

Canada confirms that if Canada requests additional measures, beyond those articulated in the Statement of Work, to safeguard personal information, then Canada may use the Task Authorization process to implement the change. While the definition of reasonable measures is a matter of interpretation by law, reasonable measures implies that a measure that can be implemented should be implemented, in the context and purpose of the Contract.

QUESTION: 304

Section 7.5.2 (f) (vi) – page 39 – under safeguarding personal information

Could the crown provide a definition of "reasonable security or protection measures"? \which types of measures would not fall under that category?

ANSWER: 304

Weak or inadequate security or protection measures that do not provide proper risk management would not fall under that category. Refer also to the answer to question #303.

QUESTION: 305

Section 7.5.2 (i) – audit

Could the crown define the meaning of "all reasonable times"?

ANSWER: 305

At "all reasonable times" means times that are acceptable to the Government of Canada within regular business hours.

QUESTION: 306

Section 7.5.2 (l) – legal requirement to disclose personal information

Could the crown acknowledge that there may be circumstances where a firm may be unable to notify the contracting authority prior to release of information to a court of law and that such occurrences will not be considered a breach of contract under these terms.

ANSWER: 306

Canada would consider these circumstances but does not rule out a contractual breach if it does occur. Canada will be reasonable in its application of the provisions in any event.

QUESTION: 307

Amendment #8, Answer 73 states *"The Contractor must develop the integration solution between EPS and the DFMS SAP instances. Furthermore, the connectivity between the SAP instances and the GC ESB will be a GC responsibility."* Does "connectivity" in this context mean that GC is building the SAP DFMS to ESB integration or does "connectivity" refer only to the ability of the SAP DFMS instances and GC ESB to communicate over the network?

ANSWER: 307

In the context of connectivity as it relates to the ESB, yes, the GC is responsible to ensure connectivity between the SAP DFMS and the ESB.

QUESTION: 308

In follow-up to Answer 80 in Amendment 9, *"Should there be additional criteria or requirements that prevent Bidders from proposing a SaaS EPS, please highlight these specific criteria..."*, Section 1.1 states that the Crown wants the selected Contractor to *"deliver, enable, implement, support, and manage a bilingual (in English and French) Government of Canada wide Software as a Service (SaaS) e-Procurement Solution"* which may indicate a single contract with the selected Bidder. In a standard approach to procuring a multi-tenant cloud solution, the Systems Integrator would deliver the implementation and management services, and the Crown would contract for the software subscription directly with the cloud software vendor. We recognize this change may require a shift in the SLA approach and may impact how terms and conditions are applied; along with our software partner, we are available to engage with the Crown to define a workable approach at its earliest convenience. Please confirm the Crown will allow for this contracting approach.

ANSWER: 308

Canada will not allow this approach. Canada is looking for a single Contractor to manage the entirety of the EPS and all related Work, as defined in the RFP.

QUESTION: 309

Section 6.13.3.1.h – Application Availability states an expected *"SLA Performance of 95% for non-production environments"*. Does the Contractor need to support any non-production environments other than one for each of Development, Test and Training?

ANSWER: 309

Please note that the SLA for non-production has been deleted. Other than the non-production environments that have been specified in the SOW, it is at the discretion of the Contractor and its proposed solution. Please also see the answer to question #213.

QUESTION: 310

Regarding B-05.04, where the requirement states "for the manual creation and publication of different tender notices including attachments to GETS for Users not leveraging EPS for sourcing activities", we have the following questions:

- i) Who will these users be? For example, could they be part of the Broader Public sector? And are these users always going to be part of some Canadian Government department or agency (at any government level)?
- ii) Will these users require future access to other EPS functionalities mentioned in the SOW section Part 3?

ANSWER: 310

i) While the ability “for the manual creation and publication of different tender notices including attachments to GETS for Users not leveraging EPS for sourcing activities” could initially be used within the GC during transition, it is primarily focused on the Broader Public Sector. Please see Annex 1 – Statement of Work, Part 7 Optional Services, section 7.3.1 Extending Access to Other Canadian Broader Public Sectors.

ii) Yes it is possible that Users will require access to other EPS functionalities.

QUESTION: 311

Page 24 of the RFP, Section 6.1 Security Requirements, For Foreign Suppliers, i. “The Contractor and any and all subcontractors must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument.” (a “NATO/EU/Bilateral Instrument Country”)

Can a Bidder that is a corporation incorporated in a NATO/EU/Bilateral Instrument country use a subcontractor that is NOT a corporation incorporated in a NATO/EU/Bilateral Instrument Country provided that such subcontractor is acceptable to the Canadian DSA?

ANSWER: 311

No, any and all subcontractors must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument.

QUESTION: 312

Page 24 of the RFP, Section 6.1 Security Requirements, For Foreign Suppliers, i. “The Contractor and any and all subcontractors must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument.” (a “NATO/EU/Bilateral Instrument Country”)

This clause is not included for Canadian Suppliers, does that mean that Canadian Suppliers can use subcontractors incorporated in a country that is NOT a “NATO/EU/Bilateral Instrument Country” (provided that such subcontractor is acceptable to the Canadian DSA)?

ANSWER: 312

No, Canadian Suppliers must also use subcontractors that are from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument.

QUESTION: 313

Page 14 of the RFP, Section 3.6.1 “As indicated in Part 6 under Security Requirements, the Bidder should provide the full address(es) of the Bidder’s and proposed individual(s) site(s) or premises for which safeguarding measures are required for Work Performance:...”

Can the Bidder use sites or premises from one of its “Team Members” in order to meet the facility clearance requirements in the SRCL? For this question, we are referring to the definition of “Team Members” on Page 338, Section 2. b, which would be subcontractors listed in Form 3 to Part 4 (B) Subcontractor List.

ANSWER: 313

The Contractor is responsible to ensure that it meets the security requirements identified in the SRCL. Any Work containing security requirements subcontracted to any entity, including the clearance of a subcontractor’s facility where required, must be approved by the Industrial Security Sector prior to the commencement of the Work.

QUESTION: 314

Page 32 Section 7.5 Security Requirements.

If a Canadian Supplier uses a Subcontractor that is incorporated outside of Canada or a province, does the Bidder need to comply with “7.5 A. Security Requirements for Canadian Suppliers” or “7.5 B. Security Requirements for Foreign Suppliers”?

ANSWER: 314

Canadian Supplier's subcontractors must comply with 7.5 B. As outlined in the RFP, they must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument.

QUESTION: 315

Page 32 Section 7.5 Security Requirements.

Please advise whether Canadian Suppliers can use a Subcontractor that is a corporation NOT incorporated in "a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or a country with which Canada has an international bilateral industrial security instrument." provided that such subcontractor is acceptable to the Canadian DSA.

ANSWER: 315

No, as outlined in the RFP, Canadian Supplier's subcontractors must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument.

QUESTION: 316

Page 32 Section 7.5 Security Requirements.

Please advise whether Foreign Suppliers can use Subcontractors that are NOT incorporated in "a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or ... a country with which Canada has an international bilateral industrial security instrument." (a "NATO/EU/Bilateral Instrument Country") even if the resources meet the requirements of the SRCL and the work location is in a "NATO/EU/Bilateral Instrument Country" and provided that such subcontractor is acceptable to the Canadian DSA

ANSWER: 316

The subcontractor must be incorporated in a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or in a country with which Canada has an international bilateral industrial security instrument and must meet the security requirements of the Contract.

QUESTION: 317

Please provide a definition of "subcontractor" as it is used throughout the RFP.

ANSWER: 317

A subcontractor to the Contractor is an entity who has entered into any subcontract at any tier to perform any part of the Work. Subcontracts are further discussed in section 06 of General Conditions 2035 (2016-04-04).

QUESTION: 318

Annex 2, E2.137 states *"The Contractor must only allow pre-approved mobile code in the PWGSC EPS thus denying any other mobile code from being downloaded and executed."* Please clarify how requirement should be interpreted in the context of the EPS project.

ANSWER: 318

GC end user devices such as desktops and laptops are locked down, thus any and all changes to GC end user device configuration is managed internally within GC to ensure conformance with the approved GC internal network security posture. All uses of mobile code within the proposed EPS must be clearly covered during the Security Assessment & Authorization (SA&A) and must be pre-approved by the GC.

QUESTION: 319

Annex 2, E2.113 indicates that management, operational, and technical security controls in place at "alternate" work sites must achieve the same objectives as those at the "main" PWGSC EPS facility. The requirement also refers to "Primary" sites. Is there a requirement to designate one or more facility to be the "Primary" or "main" facility, and can there be more than one main facility?

ANSWER: 319

The security requirements identified within Annex 2 apply to all facilities throughout the term of the Contract. Canada does not have a limit on the number of sites, primary, main or otherwise. Please see the "Changes" section of this RFP amendment which restructured E2.113 for clarity.

QUESTION: 320

Annex 2, E2.76 states "*The Contractor must test the Incident response process for the EPS at least annually*". Does this necessarily require a distinct testing exercise, or can this requirement be met by annual audits of actual responses to detected incidents?

ANSWER: 320

This requirement can be met through 3rd party independent annual audits, provided that these audits cover the scope of services with respect to incident response as detailed in the RFP. A distinct testing exercise is not required.

QUESTION: 321

Annex 2, E2.81 indicates the Contractor must open a security incident ticket within five minutes of notification by either the Contractor or PWGSC. Does this service level also apply to PWGSC systems that will interface with the EPS and will PWGSC inform the Contractor of an incident and its potential impact on EPS within 5 minutes of its detection?

ANSWER: 321

The security requirement E2.81 requires the EPS Contractor to only open a security incident ticket within five (5) minutes of notification by either the Contractor or PWGSC. With respect to the PWGSC systems, PWGSC uses the GC's risk management framework that includes incident response for security incidents on PWGSC systems. As applicable, PWGSC systems security incident notifications are distributed in a timely fashion to all partners, including both internal and external partners.

QUESTION: 322

Attachment 2 to Part 4: Technical Evaluation, Section 4, R1.1, Section B (p 346). Section B "(b) the time period that the solution was operational and being used by the client (start and end dates)". What time period would be required in order to support a Score of 5 using Scale 1?

ANSWER: 322

The evaluation of criterion R1.1, section B is based on evaluating all of the projects on their similarity and relevance on all of the elements from (a) to (j) using Scale 1. The longer the time period the solution was operational, the more positive of a factor it will be in the evaluation of element (b) under section B. The final score for Section B will be determined by giving a single score for all of the projects combined.

QUESTION: 323

In regards to the restrictions to rates place on Annex 3 – Table 3, we request that Canada consider removing the requirement for junior level architects. It is our experience that, generally, they do not exist and that clients typically prefer Senior Architects. As such, would Canada please consider removing the requirement for junior skill sets for all resource categories where the category includes architect in the title.

ANSWER: 323

In Canada's experience, junior level resources are available and may be required by Canada. Therefore, the requirement will remain unchanged.

QUESTION: 324

Requirement E2.70 for Incident Response requires that the Contractor must automatically provide Incident Ticket information by secure e-mail to a pre-defined distribution list for each PWGSC EPS for Incidents where PWGSC specifies:

- a) information from Incident Ticket;
- b) frequency of e-Procurement updates;
- c) distribution lists, and
- d) criteria for selecting Incidents (severity, priority, content of Incident Ticket).

Does PWGSC currently utilize a PKI system issuing S/MIME enabled user certificates to allow for secure e-mail exchange between the IaaS domain and PWGSC's specified domains? If so, would Canada extend its PKI System to establish a trust with the PKI in the Bidder's EPS Solution?

ANSWER: 324

Yes, GC currently utilizes a PKI system issuing S/MIME enabled user certificates to allow for secure e-mail exchange. Canada will provide its PKI credentials to the EPS Contractor's SOC/Incident Management resources in order to secure the e-mail exchange between the Contractor's domain and the GC.

QUESTION: 325

Requirement E2.159 for Governance and Risk Management requires that the PWGSC Contractor must have an Information Security Management Program (ISMP) developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program must include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:

- a) Risk management
- b) Security policy
- c) Organization of information security
- d) Asset management
- e) Human resources security
- f) Physical and environmental security
- g) Communications and operations management
- h) Access control
- i) Information systems acquisition, development, and maintenance

Can PWGSC please clarify if the ISMP needs to be based on CANRAMP, ISO 27001, or another standard?

ANSWER: 325

The ISMP is not required to be based on a specific standard. The ISMP may be based on industry standards such as ISO 27001 or another standard, but the ISMP must include details with respect to the areas identified within E2.159.

QUESTION: 326

Regarding Answer to Question 80 from Amendment 009, can PWGSC confirm that logical separation is adequate across the environment, including storage and the security management zone/SOC?

ANSWER: 326

Canada confirms that a logical separation is acceptable across the environment, including storage and the security management zone/SOC, as long as it demonstrates compliance with the applicable requirements of Annex 2 – Security and Privacy.

QUESTION: 327

With respect to R5.6 (i) where it states "The strategy for continuous monitoring based on defined risk tolerance", please provide the specifics for Canada's "defined risk tolerance" such that bidders can plan for and cost appropriately.

ANSWER: 327

The technical criteria requirement R5.6 (i) has been amended and the "risk tolerance" removed. Additionally, "for the defined measures" has also been removed from R5.6 (iii). Please see the "Changes" section of this RFP amendment.

QUESTION: 328

Reciprocal to section 10.23.2 where the Contractor must provide at least 12 months notice in advance of discontinuation of the EPS, would Canada provide 12 months notice to the vendor in the event that Canada opts to discontinue the service.

ANSWER: 328

With regards to section 10.23.2, as the EPS will no longer be provided after the Term of the Contract, this section is being revised. Please see the "Changes" section of this RFP amendment. As per section 7.7.2 Option to Extend the Contract, "(...) *Canada will send a written notice to the Contractor at least 6 months before the expiry date of the Contract*", notwithstanding all of Canada's rights and remedies allowed under the Contract.

QUESTION: 329

Please provide list of procurement data object types that are considered Open Data that need to be published to Open.canada.ca.

ANSWER: 329

Please see the answer to question #290 f).

QUESTION: 330

Please confirm whether the Crown can provide access to a GC furnished Service Desk tool. If so, what would be the cost to the vendor?

ANSWER: 330

Canada confirms it will not provide a Service Desk tool as GC furnished equipment.

QUESTION: 331

Does all EPS functionality need to be provided by COTS products, or is it acceptable that certain functionality is delivered using custom development?

ANSWER: 331

Whether it's through the use of COTS or customized products, the Contractor is responsible to deliver all functionalities described in the RFP. While Canada's preference is for all functionalities to be delivered by COTS products, Canada recognizes that some functionality may need to be delivered using custom development.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.