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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St./11, rue Laurier
Gatineau
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.** 019
Client Reference No. - N° de référence du client 20131350	**Date** 2016-08-15
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 2016-09-19**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: 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**	

Canada

Request for Proposal (RFP)

Solicitation Amendment: 019

Purpose:

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

(A) CHANGES

CHANGE: 125

Delete section *5.4.4 IT Security Certifications* of *Annex 1 - Statement of Wor*k in its entirety and replace with:

5.4.4 IT Security Certifications
The Contractor must maintain any certification and audit standards, provided as part of its bid, during the entire Term of the Contract.

Prior to enabling any credit card processing through EPS, if applicable, the Contractor (and/or their sub-contractor) must provide a valid PCI DSS Level 1 certificate and must maintain the PCI DSS Level 1 certification throughout the entire period in which credit card processing occurs through EPS.

CHANGE: 126

At Annex 1, section *3.5 SECTION D - PROCUREMENT MANAGEMENT*, sub section *3.5.6 Requirements*, delete requirement D-19.05 in its entirety.

CHANGE: 127

At Annex 1, section *4.4 EPS TECHNOLOGY REQUIREMENTS*, sub section *4.4.2 Technical Requirements*, delete requirement Tech.23 in its entirety.

CHANGE: 128

At Annex 1, section *6.13.3.2 Reporting*,

DELETE: This service level identifies the adherence of the Contractor to the agreed schedule and accuracy of reports, as identified in the SO.

INSERT: This service level identifies the adherence of the Contractor to the agreed schedule and accuracy of reports, as identified in the SOW.

CHANGE: 129

At Annex 1, section *6.10.1 Milestone #1 - Operational Planning*,

DELETE: g) Organizational Change Management Strategy as described in section 6.7.1 of the SoW; Plan

INSERT: g) Organizational Change Management Strategy as described in section 6.7.1 of the SoW;

(B) QUESTIONS

QUESTION: 399

Canada has provided an option for Bidders to use a 3rd party payment card service provider. If that payment card service provider is PCI-DSS certified for Level 1 and is located in Canada, would they have to meet all of the SA&A controls as well, and be registered in the Industrial Security Program? Or is it sufficient for the Bidder and the interfaces to/from the payment card service provider to be compliant?

ANSWER: 399

For clarity, the Contractor is not required to provide a 3rd party payment card service. Please see response to question #401 clarifying Canada's requirements regarding credit cards.

If a Bidder's proposal includes the processing of credit cards through EPS via 3rd party payment card service provider, the 3rd party must be registered in the ISP if it has access to protected information and the 3rd party payment card service provider must maintain a valid PCI DSS Level 1 certification throughout the entire period in which credit card processing occurs through EPS.

If the Bidder offers the service and it is accepted by Canada, the Contractor must perform the service.

QUESTION: 400

Due to the number of clarifications and amendments to scope received so far, could PWGSC distribute a revised RFP?

ANSWER: 400

Please refer to the response for question #416.

QUESTION: 401

Regarding the Answer to Question #112 from Amendment 11 dated 2016-06-20, we have a two part question as follows:

Part A: We request clarification on the following:

a) Regarding payment transactions, is it the expectation of Canada that the EPS solution:
i. Will process the payment transactions internal to the solution and deliver the funds to each supplier? Or
ii. Will transfer the credit card information to the supplier along with the order and total amount so that the supplier can process the payment outside of the EPS solution?

b) Industry payment card services companies or PCI DSS certified hosting environment are not typically participants in the Canadian Industrial security program. Instead, they operate under the security assurance provided in industry under the Payment Card Industry Data Security Standard. If the bidder is proposing a model that uses a 3rd party payment card service or a PCI DSS certified hosting environment, would they be considered an external service provider exempt from the subcontractor security criteria in the RFP (i.e. the Industrial Security Program)?

Part B. Regarding Section 3.7, requirement F-03.06 states that there could be connectivity to Supplier's backend systems for transmission of Invoices and Credit memos using EDI or Web Services. When that level of Supplier connectivity is done, Suppliers also request Purchase orders be sent with the same method to their backend systems. Could Canada confirm whether Purchase Orders transmission to Supplier backend could also become a future requirement for EPS? And if yes, which of the above a) or b) (of Part A question above) would be applicable in this scenario?

ANSWER: 401

Part A:

Please note that the subject requirement A-08.04 of Question and Answer #112 has been deleted as per the revised SoW in Amendment 18 and D-23.00 Card Management was added to provide clarity regarding Canada's requirements pertaining to ghost cards and user specific acquisition cards.

In accordance with D-23.04, the EPS must send card payment information along with the order so that the supplier can process the payment outside of the EPS with their credit card service provider. Masked card information (such as a few digits of the credit card, expiration date, source of credit card) is sufficient to meet this requirement. The EPS is not required to process payment transactions and deliver funds to suppliers.

For non-credit card payments, the DFMS and the Receiver General's SPS systems will continue to process payments and issue funds to suppliers as is currently being done today. In accordance with requirement A-08.05 of the SOW, all relevant receipt of goods/services and payment information must be reconciled between EPS and the DFMS.

b) Please see the response to question #399. Canada notes that given the variety of government programs leveraging credit card services, payment card services companies are in fact participants in the Canadian Industrial Security Program.

Part B:

Canada confirms that Purchase Orders transmission to a supplier backend is not a requirement of this SOW. However, if a supplier requests the Contractor to enhance their functionality, the cost of the modification must not be borne by Canada.

QUESTION: 402

In regards to the following RFP requirements, D-19.05, A-08.04, H-01.16, J-03.01, Tech.23 (comply with PCI-DSS as a Service Level 1 Provider), PCI Data Centre Compliance as stated on page 267 # 3rd requirement in the table, R5.7, Section 1.4 on PCI-DSS certifications, we believe that eProcurement applications by their nature do not store credit card information within the Application. eProcurement applications typically store masked credit card information such as a few digits of the credit card, expiration date, source of credit card. We believe this is sufficient to transact on Purchase orders between the client and suppliers. The real credit card information is private between the client and supplier and as such the payment vehicle for credit card storage and processing should be outside of these requirements. We believe that EPS should simply be the maintainer of payment method types such as indicated in D-03.15 with masked credit card information as described above. Therefore, we kindly request the removal of all credit card storage and payment processing requirements from this RFP's requirements as per reference to all requirements mentioned above.

ANSWER: 402

Please see response to question #401 clarifying Canada's requirements regarding credit cards. Regarding the request to remove requirements pertaining to credit card storage and payment processing:

- Please see the changes section of this amendment deleting D-19.05
- A-08.04 has been deleted as per the revised SoW published in Amendment 18
- H-01.16 will remain as it pertains to joint ventures and not credit card details
- J-03.01 will remain following the clarification in Canada's response to question #401 regarding the acceptability of masked card information
- Please see the changes section of this amendment deleting Tech.23
- Regarding *"PCI Data Centre Compliance as stated on page 267 # 3rd requirement in the table,"* please see the changes section of Amendment 18 moving Service Level Agreements from section III of Annex 2 to Attachment 1 to Part 6 – Service Level Agreements - Security & Privacy. It has been clarified that this attachment have been identified only as guidance to the Contractor for consideration;
- R5.7 will remain unchanged as PCI-DSS certification will be considered in the overall security strength of the proposal for the purpose of evaluation.

QUESTION: 403

3.3.3 Portal Requirements B-01.01

Please provide what types of content are referred to in the requirement "for Authorized Administrators to electronically and in Near Real-Time create, edit, view, approve and publish content in the Portal." Does this refer to content related to a particular tender or opportunity, or does it refer to general content such as FAQs.

ANSWER: 403

3.3.3 Portal Requirements B-01.01 refers to general content. Please note the change to B-01.01 in Amendment #018 revising the requirement to “for Authorized Users to electronically and in Near Real-Time create, edit, view, and publish content in the Portal.”

QUESTION: 404

Amendment 13, Change 60, 6.10.2 Milestone #2 - Solution Environment
The requirement b) states that "The Contractor has delivered the work and objectives described in Part 5 Non Functional Requirements". However, some Part 5 requirements are only available during future milestones and won't be available at the time of environment set ups. For instance, requirement for 5.6 Service Desk, won't be fulfilled until Milestone #3 and later, when EPS applications are delivered. Request the Crown to further assess Milestone #2, and provide specific requirements under Part 5 that are to be fulfilled as part of Milestone 2.

ANSWER: 404

Please see the changes to the SOW in Amendment #018 moving the delivery of the work and objectives described in Part 5 Non Functional Requirements to Milestone #3 – Supplier Enablement.

QUESTION: 405

6.8.1.4 User Acceptance Testing (UAT)
The RFP has stated that "Upon receiving each release, the GC will promptly perform UAT in accordance with the applicable acceptance criteria, and will inform the Contractor of the outcome of such testing." Is it required that the contractor provide testing management tools for UAT to facilitate and manage the UAT, for instance, for test scripts and plan management, test execution management, and defect management? We'd like to request the Crown to provide these testing management tools to allow easy access by the PWGSC users and to retain relevant documentations related to these tests. We further request the Crown to provide the same testing tools to the EPS project for system integration tests so that test scripts and plan can be re-used for UAT, and various testing cycles can be integrated.

ANSWER: 405

Canada does not require the Contractor to provide testing management tools to manage the UAT process though Canada is open to Bidders proposing the use of their (shared) testing management tool through their Integration and Testing plan as described in section 6.8.1.3 Transition Integration and System Testing, Annex 1 of the Statement of Work.

Information on the Canada’s UAT test processes and methods will be communicated to the Contractor following contract award. Should Canada decide to use its own UAT test management tool, Canada does not anticipate it will be in position to share it with the Contractor.

QUESTION: 406

Amendment 13, Change 72, k) Departmental Financial Management System instances
Please provide version number of SAP R3 instances and Oracle instances, including software version and patch numbers.

ANSWER: 406

For security reasons, Canada will only provide specific details regarding the software version and patch numbers for the DFMS instances to the EPS Contractor following contract award. Canada can confirm that all SAP R3 instances are on version ECC6 (ERP6) and that Canada is in the process of ensuring all SAP instances have deployed EHP6 (or higher). Bidders are reminded that in accordance with the response to question #364 in Amendment #017, they must bid on the basis that, in accordance with section 4.3.2.4 of the SoW, connectivity between EPS and DFMSs must be through the ESB.

QUESTION: 407

4.3.2.3 Technical Interoperability
The RFP states that "The EPS must interoperate with GC’s IT stack (i.e. infrastructure and platform) without significant change to the existing GC infrastructure or changes to desktops." In order to integrate EPS solution with GC's ERP systems, it is possible that certain software components or plug-ins need to be installed on GC's ERP systems, and/or certain GC's ERP systems may need to be upgraded into certain patch levels. Please confirm that the Crown will provide the necessary services to fulfill these pre-requisites for EPS.

ANSWER: 407

The EPS must work within the GC environment described within this RFP. Should there be a need for additional software, plug-in or upgrades to GC systems, Canada will assess and if applicable, will addressed by Canada or through task authorization process. If Canada is not in a position to deploy the requested change to GC systems then the Contractor will be responsible to deliver a workaround to ensure that EPS meets the requirements of the Contract.

QUESTION: 408

4.3.1 Background
The RFP states that "The PWGSC standard tool for interoperability between back office systems and business processes is the Oracle Enterprise Service Bus (ESB)." Since GC owns the Oracle ESB, please confirm that the Crown will take care of any work required to integrate between Oracle ESB and backend systems, including software, hardware, and configuration and development requirements, under the advisement and support from the contractor.

ANSWER: 408

Please refer to the answer to question #363.

QUESTION: 409

As part of the EPS project execution, several project management tools would be required. For instance, a collaboration tool such as Sharepoint to store project documentation, and an email systems to interact with GC's stakeholders and schedule meetings. With the consideration of GC's stringent security requirements, and for ease of managing this project together with GC, we recommend that these project management tools be provided by GC. Please provide a list of software and tools that GC can provide to the project team for the delivery of this project.

ANSWER: 409

PWGSC does not currently use project management or collaboration tools that can reasonably be shared with the Contractor. Canada is investigating the possibility of acquiring and sharing such tools with the Contractor. The GC will also consider the use of Contractor managed shared project management or collaboration tools if made available by the contractor. Any shared project management or collaboration tool (either GC or Contractor managed) will not be permitted to contain protected or sensitive information unless such tool meets Canada's security requirements. The Contractor would be responsible for the cost of licenses for contracted resources using the shared tools, if applicable.

QUESTION: 410

Canada's response to Q319 in Amendment 14 states: "*The security requirements identified within Annex 2 apply to all facilities throughout the term of the Contract."* To clarify, does that mean that all security controls apply to all environments and facilities, even in instances (e.g. Test, Dev) where it is not part of the IAAS Production or DR environments and no user (e.g. GC or supplier) data is stored or processed in any way?

ANSWER: 410

The security requirements identified within Annex 2 apply to all facilities that store, process and manage GC Data throughout the term of the Contract.

QUESTION: 411

GETS deployment and availability has been moved to a new Milestone #8 as per Amendment 13, Change 60. Since this Milestone has to be reached within 36 months of Contract Award, it is our understanding that GETS will need to be deployed, configured and integrated within Milestone #8 and will not be part of the EPS environment being deployed as part of Milestone #2. Please confirm.

ANSWER: 411

Please see the changes section of Amendment #018 clarifying that a GETS environment, if applicable as a distinct and separate environment from the EPS, is not required under Milestone #2.

QUESTION: 412

Section 1.6 states "The EPS must be hosted as a cloud-based solution and the Contractor must ensure data segregation of the GC's data." As described during the ITQ process we intend to propose a solution that includes a Supplier-facing interface that is common (with some ability to brand) for all clients of the multi-tenant cloud application; all tenders provided through that interface are available to anyone accessing the common site, and those tenders are stored in a common multi-tenant data repository. Please confirm that this approach is acceptable to the Crown.

ANSWER: 412

Canada confirms that when Canada's Data (such as tender data) enters a state of unprotected and publicly accessible (such as when tenders are posted), such data may reside in a common multi-tenant data repository provided the integrity of data is maintained at all times. The Contractor must ensure that Protected Data (such as a Bid) received in response to data residing in a common multi-tenant data repository must meet the segregation and security requirements of the SoW and Annex 2.

QUESTION: 413

The substantial number of mandatory security requirements prevents any multi-tenant cloud solution from being compliant. The multi-tenant cloud solution we intend to propose adheres to international security standards similar to those described in the RFP however, the solution is not compliant as it does not explicitly conform to Canadian ITSG-22 or ITSG23 standards. During the vendor meeting on May 3, 2016, the Crown explained the security requirements were derived from at least three different standards and confirmed that the Crown did not expect Bidders to be 100% compliant. The suggested approach was the Crown would evaluate the winning Bidder against the requirements and identify gaps. The Crown would then work with the vendor to address the gaps to the government's satisfaction, and if a suitable accommodation is not possible the Bidder would be disqualified. This approach results in significant risk for the Bidders and we suggest that it is not in the best interest of the Crown to allow for non-compliant bids that will be considered compliant based on a post-award agreement. We, therefore, suggest the Crown either:
a) Confirms that adherence to international security standards is sufficient to satisfy the mandatory requirements and that alignment of those international standards with the ITSG standards will be confirmed through a "crosswalk" documentation exercise to be conducted during the SA&A process. Any significant gaps between the implemented standards and the Crown's expectations can then be addressed based on a joint agreement between the Crown and the Contractor.
or
b) Change the security requirements from mandatory to rated.

ANSWER: 413

a) To clarify, compliance to the security requirements of the RFP is required, however Canada confirms that adherence to international security standards that demonstrate conformance to the Annex 2 security requirements during the SA&A process supported by evidence artefacts will be acceptable. Additionally, the "Crosswalk" documentation to confirm the alignment of international standards with Annex 2 security requirements including ITSG standards will be conducted during the SA&A process based on the Contractor submitted SA&A evidence artefacts. Any and all risks associated with the significant security gaps identified during the SA&A process will be assessed by Canada and remediation action(s), deemed as required, will be communicated to the Contractor to action.

b) Canada confirms no change to the security requirements from mandatory to rated.

QUESTION: 414

Amendment 13, Answer 198 refers to *"..two additional DFMS instances (in addition to PWGSC) as described in paragraph k) of section 1.3 of Annex 1…"* however that paragraph only lists the various DFMS instances it does not state which two are included in the Fixed Fee Amount. Please clarify which two DFMS instances are in scope for the Fixed Fee Amount.

ANSWER: 414

Please refer to the answer to question #415.

QUESTION: 415

Amendment 13, Answer 198 refers to both departments *"…in two additional departments…"* and DFMS instances *"…within two additional DFMS instances…"* please confirm whether the scope to be included in the Fixed Fee Amount is the deployment of two additional departments or two DFMS instances, which could involve multiple departments.

ANSWER: 415

For clarity, following the delivery of Milestone #7, Canada intends on invoking the option to deploy EPS to up to two additional DFMS instances, as identified and requested by Canada, in accordance with 7.2.7 Government Wide Deployment – DFMS Instance Transition-In. The costs associated with the deployment to the two additional DFMS instances should be included under *Table 6.1: Optional Work - DFMS Instances for EPS* of *Annex 3 - Price Schedule, version 3.0* and should not be included under the fixed fee.

QUESTION: 416

Given the number of changes that have been made to the RFP, we respectfully request the Crown provide an updated RFP document that includes all changes to date.

ANSWER: 416

Canada has provided a revised *Annex 1 - Statement of Work* in Amendment #018, however Canada does not intend on issuing an updated RFP document.

QUESTION: 417

Annex 3, Table 6.1 indicates the Bidder should submit a price per DFMS instance. Amendment 13, Annex 1, Section 7.2 indicates the scope of work for each DFMS instance includes the deployment of EPS to all departments associated with the DFMS instance. Given the significant scope of work expected for each department, including setup, training, and other change management activities we expect this work to be a substantial portion of the overall work for each DFMS instance. Please confirm the per DFMS pricing should assume deployment of all departments that are using that DFMS instance.

ANSWER: 417

Canada confirms that the scope of work for each DFMS instance includes the deployment of EPS to all departments associated with the DFMS instance.

QUESTION: 418

We plan to propose a multi-tenant cloud solution from a leading software provider whose technology infrastructure includes extensive NOC and SOC capability. Please confirm that where a Bidder is proposing a cloud solution that includes SOC/NOC functions that capability does not need to be replicated by the Bidder provided that those functions address the purpose articulated in the Crown's requirements.

ANSWER: 418

Canada confirms that where a Bidder is proposing a cloud solution that includes SOC/NOC functions, that the capability does not need to be replicated by the Bidder, provided that the SOC/NOC capability includes the scope of EPS services and conforms to Canada's requirements as articulated within the RFP, including, but not limited to the Security Requirements Checklist (SRCL), throughout the term of the Contract.

QUESTION: 419

Regarding Q&A #198 from Amendment 13 where it states that "*Following the delivery of Milestone #7 the Contractor must deploy the fully operational EPS in two additional departments (in addition to PWGSC)…*"; however, the response to Question #206 states that the "*Transition-In should contemplate the deployment of Contract and Sourcing Management within PWGSC and two additional instances only…*". Please clarify the services to be deployed for the additional 2 DFMS instances.

ANSWER: 419

Please refer to the answer to question #415 clarifying the requirement.

QUESTION: 420

Regarding Change 60 from Amendment 13, we don't see any details on the requirements for the deployment of the 2 DFMS instances in any of the Milestones listed. However, the response to Question #206 states that the "*Transition-In should contemplate the deployment of Contract and Sourcing Management within PWGSC and two additional instances only…*". Therefore, we have the following questions:

a) If the 2 DFMS instances are to be deployed during the Initial contract period and after completion of Milestone #7, please confirm the timeline during which the two additional instances are to be deployed.

b) Also, can PWGSC confirm that they will identify the 2 DFMS instances within a specific period of time after completion of Milestone #7 (e.g. within 6 months)?

ANSWER: 420

Please refer to the answer to question #415 clarifying the requirement. In accordance with 7.2.8 Government Wide Deployment - DFMS Instance Operational, "*for the applicable DFMS instance requested, the above elements must be completed within twelve months of Canada's request*". Canada anticipates that for planning purposes, the DFMS instances may be identified in advance of the completion of Milestone #7. However, at this time, Canada will only confirm that it may exercise the option to transition-in the 2 DFMS instances during the Term of the Contract.

QUESTION: 421

Regarding Change 72 from Amendment 13, we understand the lists were provided to better understand the user scope of the 2 Additional DFMS instances and for the remaining DFMS Optional services, however could PWGSC confirm that there is no requirement to have separate workflows, separate accounting structure, user data segregation or process flows deployed as part of the fully operational baseline EPS deployment and that these will be part of the work to be completed as part of the deployment of the optional DFMS instances?

ANSWER: 421

Please refer to the answer to question #415 clarifying the requirement.

QUESTION: 422

Regarding the deployment of the 2 additional DFMS instances (Q&A 198 from Amendment 13), could PWGSC please confirm whether the Contractor will be responsible for dealing with the 2 departments directly or will that be done through points of contacts within PWGSC?

ANSWER: 422

The Contractor's services in supporting Canada in the Government Wide Deployment - DFMS Instance Transition-In must be in accordance with the Work described in the SoW and the plans as identified in 7.2.7 f). Canada will facilitate and support the on-boarding of GC departments and agencies to the EPS in accordance with the plans and anticipates a collaborative approach to the management of the transition-in in partnership with the participating department.

QUESTION: 423

Amendment 18 introduced a new Statement of Work that fundamentally changes many aspects of the RFP, particularly to the functional requirements. The impact of these changes will take a significant amount of time to assess, examine in light of the solution we had been planning to propose, and adjust to meet the new requirements. We respectfully request a four week extension, and we ask that this request be addressed in the next week, or we will not be in a position to respond to this RFP.

ANSWER: 423

Canada extends the closing date of the RFP to 2:00 PM (EDT) on September 19th, 2016.

QUESTION: 424

As indicated through previous communications, we anticipate Bidders will require a minimum of 6 weeks to respond once PSPC has answered all compliance-impacting questions. Amendment 18 addressed several of these questions however some are still outstanding, and we will be submitting new ones in follow-up to recent responses. Please confirm that PSPC will continue to extend the RFP close date as these important questions, and relevant follow-ups, are addressed.

ANSWER: 424

Canada extends the closing date of the RFP to 2:00 PM (EDT) on September 19th, 2016.

QUESTION: 425

Given the importance of some of the outstanding questions, we request an extension to Sep 16th.

ANSWER: 425

Canada extends the closing date of the RFP to 2:00 PM (EDT) on September 19th, 2016.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME