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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
E Post Connect

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
Informatics Professional Services - EL Division/Services professionnels en informatique - division EL
Terrasses de la Chaudière 4th Floo
10 Wellington Street
Gatineau
Québec
K1A 0S5

Title - Sujet IT Security Risk Management Service IT Security Risk Management Services	
Solicitation No. - N° de l'invitation 47419-193674/A	**Amendment No. - N° modif.** 004
Client Reference No. - N° de référence du client 1000343674	**Date** 2021-04-30
GETS Reference No. - N° de référence de SEAG PW-$$EL-642-39261	
File No. - N° de dossier 642el.47419-193674	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-05-10 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Huot(642el), Alain	**Buyer Id - Id de l'acheteur** 642el
Telephone No. - N° de téléphone (819) 665-7395 ( )	**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

This Solicitation amendment no. 4 is raised to reply to bidders questions.

Question 41

Amendment 1, for CM.3 adds the following item #5, allowing firms to map similar experience to a specific category:

CM.3 5. For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified at Section 3, in Appendix A to Attachment 3.2.

However, the tasks specified in Section 3 Appendix A to Attachment 3.2 for Workstream 1, for certain categories, include very specific technology that is otherwise not required as part of the evaluation and does not represent the specific category but rather types of projects, which is inconsistent with the CM.3 requirement.

To give a fair chance to firms who are mapping similar categories, we respectfully request the following amendment for Stream 1 mapping of the IT Security R&D Specialist and the IT Security VA specialist:

SECTION 3: DETAILS DES RESSOURCES		
Resource Category and level	**Equivalent Resource Category (as it appears in the referenced contract)**	For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified below;

IT Security Research and Development Specialist		**Perform the following services for the same or similar technology specified below**:
		• Evaluate Identity & Access Management (IAM) security Program Risks around IAM Roadmap's projects, phases, and dependencies and develop standards, guidelines and procedures for an IAM Program;
		• Perform IT security review, analysis and deployment of IT solutions and implementation plans, including but not limited to, **one of** the following services/requirements:
		  • Network and application architectures;
		  • SAP and IBM WebSphere Portal technologies; and
		  • CA Technologies Identity Suite technologies.

IT Security Vulnerability Analysis Specialist		• Conduct Vulnerability Assessment (VA) testing which includes **one of the following, or similar:**
		  • Network-level VA scanning of an environment without administrative credentials;
		  • Network-level VA scanning of a sample of servers and workstations in an environment to identify OS/Office configurations issues as well as all missing patches in the platform and third party software;
		  • Application-level VA scanning in an environment of select applications including web-applications and thick-clients;
		  • Review of the architecture employed in an environment including a review of zoning and

		access policies enforced through firewall rules and any other forms. • Provide advice and guidance regarding IT security technical safeguards, existing or occurring security events, system attacks, technology changes that affect system security safeguards.

Answer 41

See AMD below

Question 42

Alternatively, can you please allow firms to map different categories either to:

- the listed tasks in Section 3 – Resource Details; OR,
- 60% of the to RFP list of tasks (section 5.0 of the SOW) for the specific category. Where CBSA is indicated in the RFP SOW tasks, this can be replace by another client name.

Answer 42

Criteria remains unchanged.

Question 43

Given the recent and unique circumstances with the current COVID-19 lockdown measures in Ontario, including school closures and remote/work from home requirements, many clients are facing a delay in gathering and coordinating the information required for this submission. Would the Crown please consider granting a one (1) week extension amending the solicitation closing date to May 7th.

Answer 43

Solicitation closes at 2:00PM on 2021-05-10.

Question 44

Amendment 001 altered Appendix A & B of Attachment 3.2 in Workstream 1 & 2 to include a column asking for "Dollar Value of Total Billable Days For Each Resource Category". It's unclear which question from Amendment 001 triggered this change / addition, can the Crown please confirm which question from Amendment 001 triggered this change / addition? We don't believe there's additional value to the Crown by inserting this requirement. Given that proponents are already demonstrating Total Billable Days for a given resource category in addition to Contract Value in Section 2 of Appendix A & B of Attachment 3.2, this should satisfy the Crown's requirement for proponents to demonstrate a large volume of billable days and contract TCV. We therefore request that the column titled "Dollar Value of Total Billable Days For Each Resource Category" from Appendix A & B of Attachment 3.2 be removed.

Answer 44

Agreed, see AMD below

Question 45

Given the provincial stay-at-home order, we have had a little bit more trouble accessing our corporate records than usual. Would Canada please consider extending the submission deadline to April 7th?

Answer 45

Solicitation closes at 2:00PM on 2021-05-10.

Question 46

For CM3, please confirm that bidders are not required to submit invoices at the time of bid submission. As noted in CM3 (both workstreams), substantiation for Minimum Billable Days will be done strictly using response template in Appendix B to Attachment 3.2

Answer 46

Substantiation for Minimum Billable Days will be done strictly using response template in Appendix B to Attachment 3.2.

Question 47

Given the complexity of this requirement, the need for suppliers to prepare and submit (2) separate and complete proposals to bid on both Workstreams, and the current availability restrictions on suppliers' employees imposed by the provincial lockdown (closure of schools etc.), would the Crown please consider an additional one (1) week extension?

Answer 47

Solicitation closes at 2:00PM on 2021-05-10.

Question 48

We are asking if it's possible to extend the closing date of bid submission due to the complexity of the bid requirements

Answer 48

Solicitation closes at 2:00PM on 2021-05-10**.**

Question 49

For both Appendix A and B of Attachment 3.2 (the RFP Billable Days Response Table), the crown is asking for "Dollar Value of Total Billable Days". This column is irrelevant to the requirement since the requirement is only asking for minimum billable days. The resource category and total billable days is relevant, but the dollar value is not. Can the crown remove this column so that bidder's won't have to compile the information?

Answer 49

Agreed, see AMD below.

Question 50

It is well known that Canada is deficient in this obligation relative to Aboriginal Set Aside procurement, see in particular the most recent article written by Chris Hannay, published 11 April 2021 (Ottawa falls short on 5-per-cent procurement promise for Indigenous-owned businesses - The Globe and Mail). In light of the federal government admittedly falling short of its mandate to allocate a specific amount of spending to Aboriginal Set aside companies, we are urge Canada to rise to the occasion.
In response to our recent question relative to ASA contract awards, CBSA's response was to also invite ASA companies to submit. This is insufficient and in no way helps to improve the situation. We would ask CBSA to reconsider its position on RFQ 47419-193674/A as it relates to ASA.

Answer 50

The requirement remains unchanged.

Question 51

In regards to CM.2 and CR.2, can the Crown please confirm (with a yes or no answer) if the following example would be deemed compliant and obtain FULL points in CR.2?

Example: The bidder presents 1 contract providing IT cybersecurity demonstrating the required activities and deliverables listed in CM.2 with a billed value of over $10M.

Answer 51

Yes, providing that the bidder has met the CM.2 criteria.

Question 52

In regards to QA#37 can the Crown please specify what information are bidders required to provide to substantiate CM.1? The Crown usually will provide a template or a list of information to be provided (e.g. contract number covering a certain period, billable information, volume of sales for IT professional service, years in business, etc.).

Answer 52

Demonstration of 8 years' experience providing Information Technology (IT) Security Consulting Services using the categories described under the TBIPS Supply Arrangement. Example of the categories listed can be found in Annex A Statement of Work

Question 53

In regards to CM.1, will the Crown accept a company profile demonstrating 8 years in business delivering IT professional services?

Answer 53

Yes.

Question 54

In regards to CM.2 can the bidder provide only one contract or is two contract required?

Answer 54

The bidder must provide (2) reference contracts.

The following changes apply to the RFP: The following changes apply to the RFP:

1. **AT ATTACHMENT 3.2 MANDATORY TECHNICAL CRITERIA**

   1.0 WORKSTREAM 1 - CYBER AND RISK ASSESSMENT SERVICES WORKSTREAM CORPORATE MANDATORY EVALUATION CRITERIA

   Please delete the Following;

CM.3 PBCP	The Bidder must demonstrate contract experience supplying ALL the Resource Categories (or equivalent resource categories under a different title), listed in the table below for the required Minimum Billable Days per category and level. To be accepted: 1) The billable days must have been for the delivery of informatics professional services; 2) For each resource category, the billable days must have occurred		

within the past 8 years prior to the bid solicitation closing date;

3) The billable days for all resource categories must have been provided under a maximum of 10 contracts;
4) The Bidder's substantiation of technical compliance should be demonstrated using the response templates in Appendix A to Attachment 3.2.
5) For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified at Section 3, in Appendix A to Attachment 3.2.

Resource Category	Minimum Billable Days per Resource Category (1 billable day = 7.5 hours)
Strategic Information Technology Security Planning and Protection Consultant	1000
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Classified)	1000
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Protected)	2000
Information Technology Security Vulnerability Analysis Specialist -	1000
Information Technology Security Research and Development Specialist	1000

Please insert the Following;

CM.3 PBCP

The Bidder must demonstrate contract experience supplying ALL the Resource Categories (or equivalent resource categories under a different title), listed in the table below for the required Minimum Billable Days per category and level.

To be accepted:

1) The billable days must have been for the delivery of informatics professional services;
2) For each resource category, the billable days must have occurred within the past 8 years prior to the bid solicitation closing date;
3) The billable days for all resource categories must have been provided under a maximum of 10 contracts;
4) The Bidder's substantiation of technical compliance should be

demonstrated using the response templates in Appendix A to Attachment 3.2.

5) For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified at Section 3, in Appendix A to Attachment 3.2.

Resource Category	Minimum Billable Days per Resource Category (1 billable day = 7.5 hours)
Strategic Information Technology Security Planning and Protection Consultant	1000
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Classified)	800
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Protected)	2000
Information Technology Security Vulnerability Analysis Specialist -	1000
Information Technology Security Research and Development Specialist	500

2.0 WORKSTREAM 2 –TECHNICAL AND BUSINESS REQUIREMENTS CORPORATE MANDATORY EVALUATION CRITERIA

Delete the following;

CM.3 PBCP

The Bidder must demonstrate contract experience supplying ALL the Resource Categories (or equivalent resource categories under a different title), listed in the table below for the required Minimum Billable Days per category and level.

To be accepted:

1) The billable days must have been for the delivery of informatics professional services;
2) For each resource category, the billable days must have occurred within the past 8 years prior to the bid solicitation closing date;
3) The billable days for all resource categories must have been provided under a maximum of 10 contracts;
4) The Bidder's substantiation of technical compliance should be demonstrated using the response templates in Appendix B to Attachment 3.2.
5) For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified at Section 3, in Appendix B to Attachment 3.2.

Resource Category	Minimum Billable Days per Resource Category (1 billable day = 7.5 hours)
System Auditor	1000
Business Continuity/Disaster Recovery Specialist	1000
Information Technology Security Engineer	1000
Technology Architect	1000
Project Manager	1000

Please insert the Following;

CM.3 PBCP

The Bidder must demonstrate contract experience supplying ALL the Resource Categories (or equivalent resource categories under a different title), listed in the table below for the required Minimum Billable Days per category and level.

To be accepted:

1) The billable days must have been for the delivery of informatics professional services;
2) For each resource category, the billable days must have occurred within the past 8 years prior to the bid solicitation closing date;
3) The billable days for all resource categories must have been provided under a maximum of 10 contracts;
4) The Bidder's substantiation of technical compliance should be demonstrated using the response templates in Appendix B to Attachment 3.2.
5) For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified at Section 3, in Appendix B to Attachment 3.2.

Resource Category	Minimum Billable Days per Resource Category (1 billable day = 7.5 hours)
System Auditor	800
Business Continuity/Disaster Recovery Specialist	1000
Information Technology Security Engineer	800
Technology Architect	1000
Project Manager	1000

2. AT APPENDIX A OF ATTACHMENT 3.2 -WORKSTREAM 1 - CYBER AND RISK ASSESSMENT SERVICES WORKSTREAM

AT SECTION 3: RESOURCE DETAILS

Please delete its entirety;

Insert the following;

APPENDIX A OF ATTACHMENT 3.2 -WORKSTREAM 1 - CYBER AND RISK ASSESSMENT SERVICES WORKSTREAM

RFP BILLABLE DAYS RESPONSE TABLE

Bidder Name: _____

To meet criterion CM.3, the tenderer must demonstrate its contractual experience in providing all categories of resources, for the minimum number of invoiced days required per category.

RESOURCE CATEGORY	NUMBER OF BILLABLE DAYS					
	Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Total Billable Days For Each Resource Category**
Strategic Information Technology Security Planning and Protection Consultant						
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Classified)						

Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Protected)						
Information Technology Security Vulnerability Analysis Specialist -						
Information Technology Security Research and Development Specialist						

Bidder Name: _____ Bidder Contract Reference #: _____

SECTION 1: CLIENT INFORMATION	
Government client (Yes/No)	
Client Organization Name	
Client Contact Name	
Address	
Telephone	
Fax (Optional)	
E-mail	

SECTION 2: CONTRACT INFORMATION	
Contract Value	
Award Date	
Expiry Date	

Description of requirement:

SECTION 3: RESOURCE DETAILS		
Resource Category and level	**Equivalent Resource Category (as it appears in the referenced contract)**	For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified below;
Strategic Information Technology Security Planning and Protection Consultant		• Develop vision papers, strategic assessments and policies/standards; • Perform Information System Security Implementation Process (ISSIP) activities for Protected and/ or information systems as identified in *Communications Security Establishment Canada (CSEC) IT Security Risk Management: A Lifecycle Approach (ITSG-33)* https://cyber.gc.ca/en/guidance/overview-itsg-33.
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Classified)		• Conduct IT security assessment and authorization (SA&A) services. SA&A services will include the analysis of systems threats, vulnerabilities, existing security safeguards and the preparation of multiple IT security artifacts; • Perform Information System Security Implementation Process (ISSIP) security activities and security assessment activities for Classified information systems as identified in *Communications Security Establishment Canada (CSEC) IT Security Risk Management: A Lifecycle Approach (ITSG-33)* https://cyber.gc.ca/en/guidance/overview-itsg-33
Information Technology Security Threat and Risk Assessment and Certification and Accreditation Analyst (Protected)		• Conduct IT security assessment and authorization (SA&A) services. SA&A services will include the analysis of systems threats, vulnerabilities, existing security safeguards and the preparation of multiple IT security

		artifacts; • Perform Information System Security Implementation Process (ISSIP) activities for Protected information systems as identified in *Communications Security Establishment Canada (CSEC) IT Security Risk Management: A Lifecycle Approach (ITSG-33)* https://cyber.gc.ca/en/guidance/overview-itsg-33.
Information Technology Security Vulnerability Analysis Specialist –		• Conduct Vulnerability Assessment (VA) testing which includes one of the following, or similar: o Network-level VA scanning of an environment without administrative credentials; o Network-level VA scanning of a sample of servers and workstations in an environment to identify OS/Office configurations issues as well as all missing patches in the platform and third party software; o Application-level VA scanning in an environment of select applications including web-applications and thick-clients; o Review of the architecture employed in an environment including a review of zoning and access policies enforced through firewall rules and any other forms. • Provide advice and guidance regarding IT security technical safeguards, existing or occurring security events, system attacks, technology changes that affect system security safeguards.
Information Technology Security Research and Development Specialist		Perform the following services for the same or similar technology specified below: • Evaluate Identity & Access Management (IAM) Program Risks around IAM Roadmap's projects,

		phases, and dependencies and develop standards, guidelines and procedures for an IAM Program; • Perform IT security review, analysis and deployment of IT solutions and implementation plans, including but not limited to, one of the following services/requirements: o Network and application architectures; o SAP and IBM WebSphere Portal technologies; and o CA Technologies Identity Suite technologies.

3. APPENDIX B OF ATTACHMENT 3.2 -WORKSTREAM 2 - TECHNICAL AND BUSINESS

Delete its entirety;

Insert the following;

APPENDIX B OF ATTACHMENT 3.2 -WORKSTREAM 2 - TECHNICAL AND BUSINESS
RFP BILLABLE DAYS RESPONSE TABLE

Bidder Name: _____

To meet criterion CM.3, the tenderer must demonstrate its contractual experience in providing all categories of resources, for the minimum number of invoiced days required per category.

RESOURCE CATEGORY	NUMBER OF BILLABLE DAYS					
	Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Cross Reference to Contract Reference # _____ Billing Period: __/__/__ (dd/mm/yy) To __/__/__ (dd/mm/yy)**	**Total Billable Days For Each Resource Category**
System Auditor						
Business Continuity/Disaster Recovery Specialist						
Information Technology Security Engineer						
Technology Architect						
Project Manager						

SECTION 1: CLIENT INFORMATION	
Government client (Yes/No)	
Client Organization Name	
Client Contact Name	
Address	
Telephone	
Fax (Optional)	

E-mail	
SECTION 2: CONTRACT INFORMATION	
Contract Value	
Award Date	
Expiry Date	
Description of requirement:	

SECTION 3: RESOURCE DETAILS		
Resource Category and level	**Equivalent Resource Category (as it appears in the referenced contract)**	For ''equivalent resources'' only, bidder must demonstrate similar resource category performed the tasks Identified below;
System Auditor		• Conduct systems under development reviews by: o reviewing project documentation; o conducting interviews; o assessing work completed; and o reporting on compliance with policy, standards and procedures, and progress against plan; • Conduct reviews of systems recently implemented and reporting on: o benefits actually achieved versus projected benefits; o features actually delivered versus stated requirements; o adequacy of controls and system security features; o user satisfaction based on surveys or interviews; and o system performance and reliability;
Business Continuity/Disaster Recovery Specialist		• Develop and implement business and technology continuity plans and develop technology, business continuity and disruption recovery strategies; • Develop techniques to identify and evaluate potential disruptions and develop, implement backup, replication and redundancy strategies as required but not limited to the following: o Develop crisis communication planning strategies; o Identify past and potential impact resulting from disruptions; o Develop DR test plans, coordinate and monitor DR testing.
Information Technology Security Engineer		• Develop detailed architecture artifacts based on business and technical requirements and provide IT engineering advice and guidance at each stage of the system development life cycle; • Provide IT security impact analysis of security work requirements to be performed. The impact analysis will: o Identify the security assessment requirements, o Level of effort (expressed in hours) to perform requirements and, o Estimate costs for the completion of the requirements;

Technology Architect		Prepare technical architectural artifacts adhering to industry best practices and ensure integration of IT security controls throughout the technical solution architectural design process, but not limited to the following: o providing technical analysis of architectural designs and the security controls applied to IT solutions; Perform ISSIP security activities and security assessment activities for Protected and/or Classified information systems as identified in *Communications Security Establishment Canada (CSEC) IT Security Risk Management: A Lifecycle Approach (ITSG-33)* https://cyber.gc.ca/en/guidance/overview-itsg-33
Project Manager		• Develop and administer project management services to support IT security business, operations and IT/IM transformation projects, prepare IT Security Risk Management Project artifacts: o Project Charter o Project Plan o Project Action Plan o Project Milestones & Cost analysis o Project Schedule o Project Objectives o Post Project Report o Develop vision papers, strategic assessments and R&D policies • Develop and administer project management services to support IT security business, operations and IT/IM transformation projects.

ALL OTHER TERMS REMAIN UNCHANGED