RETURN BIDS TO :

Shared Services Canada / Services partagés Canada

C/O Andrew Nimmo (Contracting Authority)

Andrew.nimmo@canada.ca

180 Kent St.,13th Floor,

Ottawa, ON, K1G 4A8

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Shared Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out thereof.

Proposition aux: Services partagés Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexées, au(x) prix indiqué(s)

Title – Sujet **Enterprise Vulnerability Management Solution**	
Solicitation No. – N° de l'invitation **15-010876/A**	**Amendment No. – N° de modif.** 0**07**
Client Reference No. – N° référence du client **15-010876/A**	**Date** **2017-01-26**
File No. – N° de dossier **019eo-2015119/A**	
Solicitation Closes – L'invitation prend fin **at – à 02 :00 PM** **on – le 2017-02-13**	**Time Zone** **Fuseau horaire** Eastern daylight standard time EDST Heure normale de l'Est HNE
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Inquiries to : - Adresser toutes questions à: Nimmo, Andrew	**Buyer Id – Id de l'acheteur** 019eo
Telephone No. – N° de téléphone : 613-668-5697	**FAX No. – N° de FAX** Not applicable
Delivery required - Livraison exigée See Herein	**Delivered Offered – Livraison proposée**
Destination – of Goods, Services, and Construction: **Destination – des biens, services et construction :** See Herein	

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
15-010876/A	007	
Client Ref. No. - N° de réf. du client	**File No. - N° du dossier**	**CCC No./N° CCC - FMS No/ N° VME**

.

Comments - Commentaires

This document contains a Security

Requirement

Vendor/firm Name and address

Raison sociale et adresse du fournisseur/de l'entrepreneur

Facsimile No. – N° de télécopieur

Telephone No. – N° de téléphone

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**

AMENDMENT # 007

This amendment is raised to:

1) Respond to the questions from bidders relating to the content of the RFP, as set out in Appendix 001;

2) Amend the Request for Proposal (RFP), as set out in Appendix 002;

Appendix 001

Question 37
For Question 20:
Please indicate the number of network element devices (physical and virtual) that are using a unique IP-address such as routers, switches, firewall, load balancers etc. Otherwise stated — Of the 300,000 devices, how many are printers and how many are network devices as described above.

Answer 37
The Crown estimates the current inventory of network element devices at 247,000 devices.
The Crown estimates the current inventory of network printers at 53,000 devices.

Question 38
Reference Mandatory requirement M6, and Canada's Amendment 001, Answer 001: Canada has confirmed in its response to Question 1 that there is not a single incumbent vulnerability scanning solution active within the SSC's environment today, but 'many legacy environments' and 'multiple vulnerability scanning solution(s)'. In addition, Canada is requesting that the Bidders solution must 'cohabitate' with these multiple solutions during a yet to be defined transition period to a centralized solution.

Currently, there are more than 50 commercial and open source vulnerability scanning tools available in the market, and approximately 35 companies offering solutions for OWASP (Open Web Application Security Project) . Unfortunately, there is no standardized format among these supplier solutions today severely limiting the import or exchange of vulnerability data between solutions with most vendors developing their solutions using their own proprietary formatting and individual patents.

We understand Canada's desire to have Bidder's supply a solution that meets SSC's mandatory requirement outlined in M6, and the benefit to transition it could provide, but this requirement is too restrictive for all vulnerability scanning vendors, and too uncertain as Canada has not provided any detail regarding the current environment.

In light of these challenges that are likely facing all Bidder's will SSC:

a) Amendment M6 from and mandatory to a rated requirement?
b) Provide SSC's proposed implementation timeline from 'cohabitation' to a centralized solution?
c) Provide a list of solutions active in the environment today that SSC would like to maintain through the implementation and transition period?

Answer 38

a) Please see forms 3 and 4 revised January 20, 2017.xls posted on the RFP webpage. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-17-00762407
b) The crown has not agreed to reword the RFP to include 'cohabitation'. The current, in place vulnerability solutions have licenses expiring in roughly 1 year. The in place vulnerability solutions will be migrated to the Enterprise solution upon renewal.
c) Please see forms 3 and 4 revised January 20, 2017.xls posted on the RFP webpage. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-17-00762407

Question 39

M2 states "A full non-credential based scan of 10,000 IP addresses must complete over a 2 day period, staggered over non-production hours to limited impact to daily operations."
Does the meaning of "full non-credential based scan" mean scanning all 65,535 TCP and UDP ports? Since UDP communication is connection-less, UDP port scans can take much longer to complete compared to TCP port scans.
What are the non-production hours per day?
Do the non-production hours vary from weekday to weekend?

Answer 39

Due to the various time zones across Canada the Crown considers non-production hours as 20:00 to 06:00 Eastern time, 7 days a week.

Question 40

M16 states "The solution must enforce a trusted/authenticated relationship with the source of vulnerability information. "

Is this asking where the software receives it vulnerability feed from?

Usually each vulnerability management software vendor will manage the vulnerability information. Is this requirement asking for the process workflow such as how each company verifies that the vulnerability information is correct?

Answer 40

Clarification: M16 relates to the trust communiques channels between the Crown and Vendor for software updates to the solution.

Question 41
M17 states "The solution must have the ability to interface with the vulnerability information from the National Vulnerability Database (NVD) for data feed sources."

What kind of interface is being expected? Is simply a reference back to the NVD sufficient for each vulnerability, or is there some additional interface required?

Answer 41
The Crown expects a link and reference details back the NVD or stated source of the vulnerability information towards every vulnerability.

Question 42
M20 - The solution must provide the ability to ensure that all logs/debugging information/memory dumps can be sanitized for sensitive information so that they may be shared for vendor support.

Could you please clarify what is considered sensitive information? Credit card numbers, IP addresses, usernames, passwords, etc?

Answer 42
The Crown considers any data that can identify the Crown, assets of the Crown or employees of the Crown as sensitive of data. User credentials, given, middle and surname of a user, passwords, IP addresses, server name, end user device name, location and credit card.

Question 43
M22 states "The solution must be capable of performing agent and agentless scanning of configuration compliance."
How many agents are expected?

Answer 43
At this time the Crown cannot estimate the number of agents that are expected. The Crown assumes that the number of agents will vary depending on the solutions proposed by the various vendors solutions on the RFP. The Crown is expecting the vendors to provide the details towards how many agents they will be biding.

Question 44
For the SSC Network included in this RFP, will this be a self-contained network or will there be external partner departments on other/their own networks that will be supported also part of this scope?

Answer 44
The Enterprise solution will be expanded to include external partner departments on other/their own networks.

Question 45

Column L & J in the first tab of the pricing sheet are not reflecting the right formulas. Can the crown please amend and resend?

Answer 45

Please refer to Appendix 002 of this Amendment

Question 46

SOW 7.2.2 is required in both the initial contract (1st tab) and optional items (2nd tab) pricing sheet. As answer to Q30, it is stated "The Crown doesn't predict inventory growth up to 2,000,000 until the end of the 5 year contract."

i. Please clarify why should growth beyond initial 2 million devices (ie SOW 7.2.2) should then be accounted for in the initial contract (1st tab)

Answer 46

The Crown requires the option to purchase additional licenses and/or hardware capacity at the original bid price set in the contract should our requirements exceed the 2,000,000 device requirements. Option to purchase an additional year of support for up to three (3) years at the original bid price. Option to buy additional five (5) day training package(s) for up to three (3) years at the price set by bid.

Question 47

Answer to Q21 states "Currently the Crown estimates have 100,000 servers and 600,000 desktop devices. A complete roll out of the solution and the scale up to 2000000 devices would be staggered over several years."

ii. Can the crown provide an estimated growth from year 1 to 5, as this can impact our pricing model?

Answer 47

The Crown requires 500,000 initially scaling up to 2,000,000 within the contract , the crown predicts an estimated 20% growth per year over the 5 year contract, growth will be covered by the 3 option years in the pricing tables.

Question 48

The pricing table does not capture any requirements for lab hardware and software (SOW 7.3.1). Can the crown clarify where we should account for this cost in the financials?

Answer 48

Please refer to Appendix 002 of this amendment

Question 49

Upon contract award, what is the crown's replacement strategy in terms of removing other vendor scanners and standardizing with the selected vendor? Please provide estimated numbers on a yearly basis.

Answer 49

SSC currently has an estimated 185 various Vulnerability Assessment scanners supporting a various numbers of IP address per license. The support renewals are done annually and will be spread across the 5 year contract. Estimate numbers towards yearly onboarding cannot be provided because the partners departments have various numbers of scanners and it would depend on what year that partner was on boarded to the Enterprise Solution.

Question 50

With regards to Common Criteria, EAL3/EAL3+ imposes some additional requirements on the vendor for documenting practices and procedures related to configuration management, development environment security, and the vendor's development life cycle model, but does not mandate any mechanisms that go beyond good commercial practice. EAL2/EAL2+ and EAL3/EAL3+ share the same level of vulnerability analysis, penetration testing and independent testing. As such, an EAL3/EAL3+ evaluation does not represent any significant increase in the security assurance provided by an EAL2/EAL2+ evaluation.

b. We are therefore requesting the crown to modify R23, to the following

"The solution must have Common Criteria certification at EAL2+ or EAL3 or higher to ensure product has been adequately tested and reviewed."

Answer 50

The Crown had already moved this requirement from a Mandatory to Rated requirement. The Canadian Security Establishment has stated that the solution has a requirement of an EAL3 rating, thus the Crown will not further lessen this requirement.

Question 51

R1:The solution should support centralized management and reporting servers which can operate independently (including their respective dependent scanners and agents), as well as be subordinate to a higher echelon of management and reporting servers. The management and reporting servers should support multiple hierarchal levels of subordinate management and reporting servers (including their respective dependent scanners and agents).

a. Can you provide more detail around the requirements for the centralized management and reporting servers operating independently? What does independence entail?
b. How many levels of subordinate management and reporting servers is SSC anticipating for the requirement hierarchies?
c. How many different hierarchies of centralized management and reporting servers are anticipated?

Answer 51

a) Independence would entail having the ability to deploy a solution to an outside partner, allowing the partner to perform all the necessary functions but have the solution rollup all information to a solution at SSC.
b) The crown cannot provide an answer because it may vary by the solution. This effort will be determined as part of the work outlined in the SOW.
c) The crown cannot provide an answer because it may vary by the solution. This effort will be determined as part of the work outlined in the SOW.

Questions 52

M4 The solution must be capable of Risk Prioritization customization based on business context. Question. Can the crown please clarify and elaborate on the meaning of business context as it relates to VMS solution.

Answer 52

The crown requires the ability to adjust the risk score in order to increase the risk prioritization on mission critical devices. The Crown would determine what devices are mission critical or required to main operations based on the function\business context of the device.

Question 53

Regarding R6, can the Government of Canada please provide more details about the requirements for "Authentication protocols to collect file" when integrating with SIEM technologies.

Is this requirement asking if there are files containing authentication logs that can be ingested by a SIEM, or is this asking for something else

Answer 53

The authentication protocols listed within the requirement will be used to integrate the solution with SSC's in place SIEM solution

Question 54

R6 speaks to the "ability to integrate with SIEM technologies." This requirement does not include several common mechanisms for integrating third party components such as a REST API, XML, ODBC/JDBC and SOAP. Please consider adding these commonly-used integration mechanisms to the rated requirements to reflect the value of these standards-based interfaces to the Crown.

Answer 54

The Crown has included the mechanisms required to interact with the currently in place SIEM(s) technologies. Bidders can list other technologies but the Crown will not be changing the scoring or the content of rated requirement 6.

Question 55

Please confirm the Crown will accept screenshots as substantiation of product functionality.

Answer 55

3.2 Section I: Technical Bid of the RFP outlines that It is the bidder's responsibility to provide the necessary information to demonstrate their understanding and substantiation to the requirements. It is up to the bidders to determine the best way of doing this.
The recommended solution will also be subject to the VCMS test plan prior to contract award. This test plan will be used to verify a subset of the VCMS solution mandatory requirements. Only the winning bid will be subjected to this test plan; if bidder fails to demonstrate the requirements to the satisfaction of SSC, the bidder will automatically be disqualified and the next eligible bid will be evaluated.

Question 56

Reference Annex B Pricing Tables, Purchase Items & Services tab, Line items 1 & 2, 2 Years Initial Contract Support.

Can SSC explain why Line Item 1/Column F includes no formula, where Line Item 2/Column F includes the formula =E10*F10?

Answer 56

Please refer to Appendix 002 of this Amendment

Question 57

Reference Annex B Pricing Tables, Purchase Items & Services tab. Our solution in response to Line 1 and Line 2 will require multiple Part Number with different quantities.

Are Bidders required and permitted to include multiple product codes in column C?

Answer 57

Yes, Bidders can include multiple part numbers, however as this is a solution the quantity should reflect the quantity required to deliver the solution of the initial requirement

Question 58

In Line 2 of Annex B Pricing Tables, SSC states that "INITIAL CONTRACT PERIOD Initial Contract Period (HW &SW) includes two (2) Years Maintenance and Support for HW and SW". If it is to be included, why has SSC separated pricing for the 'Firm Lot Price' from the '2 Years Initial Contract Support' in columns E & F? Or are these two separate requirements?

Answer 58

It is the same requirement, Support Cost and Solution Cost are treated differently internally (Capital vs Expense) when procuring so as such they are broken out, the 2 years support in Column F is the Support required for the Solution detailed in Column E.

Question 59

In Annex B Pricing Tables, Column D, the quantity listed is preset to 1 (one). Is SSC permitting Bidders to correctly represent quantity of product codes greater than 1 (one) needed to meet the minimum requirements for SOW 7.2, 7.7.2. and 5.1.2.?

Answer 59

Yes, Bidders can include multiple product codes greater than 1 (one), however as this is a solution the quantity should reflect the quantity required to deliver the solution of the initial requirement.

Question 60

Shared Services Canada has released the Request for Proposal for an Enterprise Vulnerability Management solution with a requested submission date set at February 6, 2017, in order to have to provide Shared Services Canada a fully compliant response, we are respectfully requesting a three week extension to the February 6th contemplated submission due date

Answer 60

The Crown has already granted a 1 week extension. The Crown can accept another 1 (one) week extension, until February 13th. Please refer to Appendix 002

Appendix 002

AMENDMENT TO THE REQUEST FOR PROPOSAL (RFP)

1.0 Amend the Request for Proposal Closing date:

From: February 6, 2017

To: February 13 2017

2.0 At PART 7 - RESULTING CONTRACT CLAUSES, Section 7.20

DELETE 7.20 Security Requirements

INSERT 7.20 Security Requirements

The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS), issued by the Canadian Industrial Security Directorate (CISD), Public Services and Procurement Canada (PSPC).

The contractor and/or its employees must maintain a valid security screening at the level of SECRET, granted by Canada and approved by Shared Services Canada.
The contractor and/or its employees MUST NOT remove any PROTECTED or

CLASSIFIED information or assets from the identified work site(s).
The contractor and/or its employees MUST NOT use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data.
Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of Shared Services Canada.
The contractor and its employees must comply with the provisions of the:
a) Justice Canada – Security of Information Act (Latest Edition);

b) Industrial Security Manual (Latest Edition)

3.0 AT PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION, 4.2 Conduct of Evaluation in Steps

DELETE b)Step 2 – Evaluation of Rated Requirements:

INSERT b)Step 2 – Evaluation of Rated Requirements:

Bids that meet all the Mandatory Criteria will then be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly. The rated requirements are described in Form of Annex C.
Bidders must achieve a minimum score of 121.5/162 on the rated requirements to be considered responsive (i.e. 75% or higher out of the overall point-rated maximum points). In all calculations, the Total Technical Score (TTS) will be rounded to two decimal places. Bids that do not score at least 121.5/162 will be declared non-responsive and be disqualified.

4.0 **DELETE** Form 3 and 4 Revised January 20 2017

INSERT Form 3 and 4 Revised January 26 2017

5.0 **DELETE** ANNEX A SOW

INSERT ANNEX A SOW Revised January 26 2017

6.0 **DELETE** ANNEX B Pricing Tables Revised January 13 2017

INSERT ANNEX B Pricing Tables Revised January 26 2017

7.0 **DELETE** Annex E Security Requirements Checklist

INSERT Annex E Security Requirements Checklist Revised January 26 2017