ANNEX A

Enterprise Vulnerability Management Solution
STATEMENT OF WORK

1. INTRODUCTION

Shared Services Canada (SSC) is a Government of Canada (GC) department entrusted with the transformation and ongoing management of the IT Infrastructure for 43 departments within the GC. This specification will describe the desired capabilities for infrastructure components to support SSC's Vulnerability Management System. Government of Canada programs and data are exposed to unknown risks due to SSC's and its Partners' lack of comprehensive visibility and monitoring capabilities within all IT environments. This impairs SSC's ability to have a comprehensive view of existing vulnerabilities and be able to take remedial actions. The GC requires effective enterprise vulnerability management services (VMS) that proactively and continuously explore and reduce risks and impacts resulting from systems being exposed, while being a key enabler to the overall risk management framework.

SSC has a requirement to implement an enterprise wide Vulnerability Management System. This is a critical prevention tool that is used on a daily basis by SSC in order to detect and confirm vulnerable assets within our infrastructure.

SSC's project scope includes the procurement, configuration and deployment of an enterprise vulnerability management tool(s) to enterprise data centres, legacy data centres, Internet facing infrastructure, and GC end points. The solution must be capable of performing asset discovery, vulnerability scans, and vulnerability reporting for up to 2,000,000 IT assets. SSC's scope also includes communications and collaboration across various groups including: vulnerability management, risk management, change management, asset management, patch management, security operations, clients, and external stakeholders.

This project also has the requirement for the design of a permanent lab infrastructure located in the NCR replicating the production environment. This lab will be used by SSC to test configurations, patches, deployments and scan templates before they are implemented in the production environments. In additional, this contract requires the delivery of a documented product-specific training package delivered by a certified OEM trainer to SSC staff.

2. TERMINOLOGY

The table below provides general information on the abbreviations that are used within this Statement of Work (SOW).

GC	*Government of Canada*
VMS	*Vulnerability Management Service*
IT	*Information Technology*
NCR	*National Capital Region*
OEM	*Original Equipment Manufacturer*
SOW	*Statement of Work*
SSC	*Shared Services Canada*
TA	*Technical Authority*

3. BACKGROUND

The GC has acknowledged the requirement to identify and address vulnerabilities in systems because these weak points are what threat actors target for exploitation. The GC has a myriad of IT systems and infrastructures spread across the globe, and current disparate vulnerability management approaches are neither feasible nor sustainable from an enterprise service offering perspective.

SSC's enterprise vulnerability management project will enable the GC to provision services to enterprise IT environments via standard offerings funded by SSC (e.g., Enterprise Data Centre scanning, IT infrastructure scanning, perimeter scanning, network scanning, etc.); cost recovered offerings funded by clients (e.g., workstation scanning); and an iterative approach for a GC-wide procurement vehicle to deliver client funded and operated Vulnerability Management capabilities.

In many cases, IT vulnerabilities are a result of previously identified or known flaws, for which patches have already been released by the vendor community. SSC's enterprise VMS will provide an overall strengthened security risk posture through awareness and comprehensive visibility into GC-wide weak points. Such knowledge will aid in proactive threat mitigation supporting overall business continuity and data safeguarding.

4. OBJECTIVES

4.1. The core objective of the contract is the procurement of an Enterprise Vulnerability Management solution to replace the existing legacy VMS infrastructure as well as augment our existing capacity and capabilities. SSC will also be expanding the solution over time to encompass more of the GC environment.

The effort will require goods and services as follows:

4.1.1. Hardware and software required to implement the solution, including;

- Capture and storage of data
- Creating reports from scans
- Performing complex security analysis of data
- Maintaining a database of assets
- Receiving vulnerability data feeds
- Receiving product updates

4.2. The second objective is the design, configuration and testing of the permanent lab environment meeting SSC's requirements that will be used as a pre-production environment to test patches, releases, configuration and scan templates before being deployed in production environments.

4.3. The third objective is to provide engineering support to Shared Services Canada. The winning bidder must provide a point of escalation where SSC can request support towards the engineering and support of the solution. For the engineering support, the professional services must be provided by the OEM either by phone or in person on a short-term as-required basis, and must be included as part of the support and maintenance provided by the winning bidder.

4.4. The forth objective is training toward the use, support and administration of the solution within the GC.

4.5. The fifth objective is for vendor-provided, short-term professional services that will be used toward the architecture, design, build, and deployment of the service**.** The professional

services provided by the bidder must be cleared at the GC Secret level, and approved and certified by the OEM.

4.6. Professional services must be included in the cost of the bid. Professional services will be used for a period of at least 60 (sixty) business days in order to aid in the architecture of the solution..

4.7. The winning bidder will be invited to perform an acceptance test to demonstrate that the bidded solution meets a subset of requirements that have been selected from the mandatory requirements by SSC. The bidder will host this testing using their own facilities, devices and product licensing. The bidder must clearly demonstrate to SSC that their solution can meet the requirements to the satisfaction of SSC. Scoring and pass marks will be assigned to each requirement. The details of the scoring and the proposed architecture that SSC wishes to see tested will be included as an annexe to the RFP. SSC will invite another bidders to participate in the acceptance testing if it is determined that the highest scoring bidder cannot meet the requirements. Mandatory aspects of the acceptance test:

4.7.1. It is preferred that the testing be demonstrated in the National Capital Region (NCR) but may be hosted through the Internet to a site in the NCR.

4.7.2. The bidder must provide physical access to the testing for 10 (ten) individuals from SSC if hosted at a lab in the NCR and up to 30 (thirty) if demonstrated via the Internet.

4.7.3. Bidder is not expected to cover travel costs of SSC individuals.

4.7.4. Post invitation to participate in the acceptance test, the bidder will have 10 (ten) days to configure their lab environment in accordance with the architecture proposed by SSC.

4.7.5. The bidder has a maximum 5 (five) days to demonstrate to SSC that they meet all the testing requirements.

4.7.6. The following mandatory requirements will be tested. Use cases as to how SSC wishes to see the testing completed is provided within the included acceptance test plan, that will be presented to the highest bidder post RFP scoring;

- M1- The solution must fully support implementation, administration, configuration and scanning for both IPv4 and IPv6 networks
- M2- The solution must be capable of performing asset discovery, inventory, tracking, and vulnerability scans of 2,000,000 network-attached IT assets. A discovery scan must record 10,000 IP addresses in one day. 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. A full credential based scan of 10,000 IP addresses must complete over a 3 day period, staggered over non-production hours to limited impact to daily operations.
- M4- The solution must be capable of risk prioritization customization based on business context.
- M6- The solution must have the ability to ingest vulnerability scan results from other vendors in various formats.
- M7- The solution must have the ability to consume and execute industry or custom SCAP 1.2 or later content.
- M9- The solution must maintain and store secure audit logs in accordance with GC policies. (See http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742)

- M11- The solution must be capable of processing, communicating, and storing data using a GC approved encryption method where deemed necessary (i.e. data sensitivity), use cryptographic algorithms, cryptographic key sizes and crypto periods that have been approved by CSE, validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) or subsequent version;
- M13- The solution must uniquely identify and authenticate organizational users through the use of Microsoft Active Directory Services.
- M18- The solution must have the ability to back up its entirety which includes but not limited to scan data configuration.
- M27- The solution must provide asset discovery, grouping, classification, and management capabilities.

4.7.7. SSC has up to 3 (three) days to review the results of the acceptance test.

4.7.8. The test will be considered a fail should the highest scoring bidder not meet the requirements or the passing mark of the acceptance test. At this point SSC will select another bidder to participate.

5. SCOPE OF WORK

5.1. The core of the contract comprises:

5.1.1. Enterprise capacity solutions and two year of maintenance and support. The solution can consist of physical network appliances, virtual servers or software, as long as they meet all mandatory requirements and the rated points as disclosed.

5.1.2. The solution must be capable to perform assets discovery scans and vulnerability scan of 2,000,000 devices at a minimum.

5.1.3. Instructor led in classroom training (maximum of 10 students) held within the NCR and possibly regional offices, consisting of 35 to 40 hours over five (5) consecutive business days.

5.1.4. The successful bidder must provide professional services in accordance with the timeframes allotted in the Objectives section. These professional services will be utilized to help deploy the solution efficiently, including:

- Engineering
- Testing
- Optimization
- System configuration
- Creation of a lab environment
- Project documentation, as required, and
- Knowledge transfer to Crown resources

6. Deliverable and payment overview

Deliverable	Evaluated Criteria	Days
Procurement of an Enterprise solution	Award of contract post-test plan verification.	5 days
	SSC Acceptance of test plan results	3 days
Permanent lab environment	Test/validation of VMS Lab Setup	10 days
	SSC provided with all source code, design documents and architecture document in printed and electronic copies related to lab fit-up	
	SSC Acceptance on VMS Lab setup	5 days
Engineering support	Provide a point of escalation	
	Provide support resources with in-depth product knowledge	
	Provide support resources with experience in implementing and architecting the product from the ground up	
	Provide support resources with experience in large enterprise deployment of greater than 2 Million IP address	
Training	Training provided to a minimum of 10 resources	
	SSC Review/Validation on VMS training	10 days
	SSC Acceptance of training provided	5 days
Architecture Design	Vendor supplied architecture design documentation	
	Review/Validation VMS architecture design	60 days
	SSC Acceptance on VMS architecture design	5 days

7. DELIVERABLES

7.1. All deliverables specified within the SOW must be submitted to the Technical Authority (TA).

7.1.1. All hardware and software included in the Enterprise Vulnerability Management solution, including all software, appliances, network adapters, and storage required to meet the mandatory requirements and meet all rated points that have been disclosed with the bid.

7.1.2. The subscription of the first 12 months of product threat feeds must be included.

7.2. The core deliverable of the contract is the procurement of an Enterprise Vulnerability Management solution to replace the existing legacy VMS infrastructure as well as augment our existing capacity. SSC will also be expanding the solution overtime to encompass more of the GC environment.

The replacement effort will require both goods and services as follows:

7.2.1. Hardware and software required to implement the solution including;

- Capture and storage of data
- Creating reports from scans
- Performing complex security analysis of data
- Maintaining a database of assets
- Receiving vulnerability data feeds
- Receiving product updates

7.3. Design, configuration and testing of the permanent lab environment meeting SSC's requirements that will be used as a pre-production environment to test patches, releases, configuration and scan templates before being deployed in production.

7.3.1. Hardware and software required to implement the solution within a lab environment

7.3.2. Professional services to design, configure and install the lab environment. The professional services provided by the bidder must be cleared at the GC Secret level, and be approved and certified by the OEM.

7.3.3. Professional services to conduct testing of the completed lab environment.

7.3.4. Professional services must provide a report signing off that the lab functions as per agreed upon requirements.

7.3.5. Professional services must provide the design documents and all related artifacts in electronic and hard copy once the lab is completed.

7.4. Engineering support to Shared Services Canada

7.4.1. Provide a point of escalation where SSC can request support towards the engineering and support of the solution. For the engineering support, the professional services must be provided by the OEM either by phone or in person on a short-term as-required basis, and must be included as part of the support and maintenance provided by the winning bidder.

7.4.2. The professional services provided by the bidder must be cleared at the GC Secret level, and be approved and certified by the OEM.

7.4.3. Provide support resources with in-depth knowledge of the product suites able to handle complex engineering level support requests.

7.4.4. Provide support resources with experience in implementing and architecting the product from the ground up to end state.

7.4.5. Provide support resources that the experience in large deployments of greater than 1 million IP address infrastructures.

7.4.6. Support must be available in both official languages.

7.4.7. Support must be available 24 hours a day.

7.5. Five (5) consecutive days of in classroom training (Maximum of 10 students) toward the use, support, and administration of the solution. Professional services related to training must be included in the cost of the bid.

7.6. Professional services will be used for a period of atleast 60 business days in order to aid in the architecture of the solution

7.6.1. Vendor provided short term professional services with a security clearance at the GC Secret level in order to design, build and deploy the solution. The professional service must be certified by the OEM of the bidded products.

7.6.2. Professional services will create the VMS architecture and design.

7.6.3. Professional services will provide all architecture, Solution architecture; detailed design, build books, support information, and design documents in electronic and printed copies.

7.6.4. Professional services will provide any customs code for this solution; including coding comments, customized scripts shall be provided to SSC in its raw format.

7.6.5. Knowledge transfer to designated Crown resource(s) as required

7.6.6. Professional services will provide all documents that were created during the build in both printed and electronic form to SSC

7.6.7. Professional services will address any concerns are questions that have not been addressed up to this point

7.6.8. Professional services will make certain that the TA and crown resources have a detailed understanding of the solution and support infrastructure

7.6.9. Professional services will provide a record on all questions and concerns that were brought up during the build and architecture.

7.7. The optional component of the contract includes:

7.7.1. Option to purchase maintenance and support for Option Years (Years 3, 4 and 5) of the equipment purchased as part of the core contract requirement.

7.7.2. Option to purchase additional Enterprise capacity hardware solutions for expansion beyond the initial 2,000,000 device requirement. 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..

8. ON-SITE PROFESSIONAL SERVICES RELATED GOODS

8.1. Resources must be available to work at GC facilities located within the National Capital Region (NCR). Computerized workstations will be provided.

Travel within the NCR will be frequent. Travel within the NCR will not be reimbursed.

8.2. The professional services resources will work under the guidance of a TA/Manager.

8.3. Status reports must be included with all invoices submitted by the vendor.

8.4. The resource will be provided with office resources.

8.5. The professional services resource must have a valid Canadian Security Clearance at the Secret clearance level. Bidder must specify security clearance file number and expiration date.

8.6. If data considered private information is handled, Professional Services must provide a service management guide for Enterprise Vulnerability Management Solution to SSC that includes privacy breach process and security breach process

8.7. If data consider private information is handled, Professional Services must provide a privacy breach report to SSC, by reporting period specified by Canada, on privacy breaches that includes: a) number of privacy incidents b) number of privacy investigations completed and C) average/highest response time t privacy incidents

8.8. Normal working hours will be no earlier than 7:00 am to no later than 6:00 pm local time Monday through Friday. The resource will be expected to work 7.5 hours/day within normal working hours, unless arrangements are made ahead of time with the TA.

8.9. The resource must be able to communicate in English effectively, both orally and written.

8.10. The resource must provide project management of ongoing IT consolidations, conversions, and transformations.

8.11. The resource must provide systems administration for any IT security system / application as required.

8.12. The resource must provide operational support for any IT security system / application as required.

8.13. The resource must perform software upgrades and apply patches.

8.14. The resource must install new or replacement equipment as required.

8.15. The resource must create and/or maintain an equipment database of equipment serial numbers and maintenance agreements as required.

8.16. The resource must test workflows with partners and peer groups as required.

8.17. The resource must maintain, create and update build and operational documents as required by workload.

9. TRAINING SERVICES RELATED GOODS

9.1. The training resource must be available to work at GC facilities mostly within the National Capital Area; however training may also be required outside of the NCR.

9.2. The training resource will work under the guidance of a TA/Manager.

9.3. The resource will not be provided with office resources, but is required to provide computing devices.

9.4. The resource is required to have a Government of Canada Reliability security clearance.

9.5. Normal working hours will be no earlier than 7:00 am to no later than 6:00 pm local time, Monday through Friday.

9.6. The resource must be able to communicate in English effectively, both orally and written. Bilingual in English and French is preferred, but not mandatory.

10. PROPRIETARY INFORMATION

10.1. Non-Disclosure

10.1.1. All work carried out by the contractor with respect to this SOW will remain the property of the Crown. All reports, documentation, and extensions thereto shall remain the property of the Crown and the contractor shall not divulge, disseminate or reproduce such reports and/or documentation to any other person without the prior written permission of the Crown.

10.1.2. All information and documents made available to the contractor during the course of this project are deemed proprietary, and shall be returned to the Crown upon completion of the tasks specified in this SOW or upon termination of the contract.

Note: Sections 11 up to and including section 14 are only applicable should the contractor and/or vendor being handling personal information. These clauses can be ignored if the vendor will not be handling personal information

11. PRIVACY MANAGEMENT PLAN

11.1. The privacy management plan demonstrates that the Contractor can meet the requirements of the Contract and provide assurance of their ability to manage Personal Information and Records in accordance with the statutory obligations.

11.2. The Contractor must provide a draft privacy management plan within 60 Federal Government Working Days after Contract award to Canada for approval. Canada reserves the right to request changes to the privacy management plan in order to ensure that privacy is being properly managed by the Contractor.

11.3. The Contractor must provide Canada with an update to its privacy management plan within 20 Federal Government Working Days of a request by Canada.

11.4. The privacy management plan must specifically describe the following items in detail:

11.4.1. Contractor's privacy protection strategies and detail exactly how the Personal Information will be treated over its life cycle;

11.4.2. how the Personal Information will be collected, used, retained, disclosed and disposed only for the purposes of the Work specified in the Contract;

11.4.3. how the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;

11.4.4. the privacy breach protocol, and details on how any privacy breaches will be handled;

11.4.5. how the Contractor intends to ensure that Canadian Privacy requirements, as outlined in the Privacy Act, the Access to Information Act and Library and Archives of Canada Act, will be met throughout the performance of the Work and for the duration of the Contract;

11.4.6. any new measures the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification;

11.4.7 how the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification; and

11.4.8 describe how the Contractor intends to ensure that their staff is trained on privacy and privacy related principals

12. PRIVACY IMPACT ASSESMENT

12.1. The Contractor must assist Canada in creating the privacy impact assessment in accordance with the TBS Directive on privacy impact assessment (http://www.tbs-sct.gc.ca/pol/docengaspx?id=18308&section=text#cha1) by providing the following information within 20 Federal Government Working Days of a request by SSC:

12.1.1 business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;
12.1.2 a list of the Personal Information used by the Contractor in connection with the Work and the purpose of each Personal Information item;

12.1.3 how the Personal Information is shared and with whom;

12.1.4 a list of all locations where hard copies of Personal Information are stored;

12.1.5 a list of all locations where Personal Information in machine-readable format is stored (e.g., the location where any server housing a database including any Personal Information is located), including back-ups;

12.1.6 a list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by the Contract;

12.1.7 any privacy-specific security requirements or recommendations that need to be addressed;

12.1.8 a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

12.1.9 results of consultations (if any) from a privacy impact assessment review by the Office of the Privacy Commissioner of Canada (OPCC) with signoff by OPCC.

12.2. The Contractor must assist Canada during the development of the privacy impact assessment and must implement recommendations from the privacy impact assessment based on a schedule approved by SSC at no cost to Canada.

12.3. - If changes to Enterprise Vulnerability Management Solution are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by the SSC, the Contractor must provide SSC with sufficient detail on the changes to support an update to the privacy impact assessment, and obtain approval from SSC Authority for the anticipated change.

12.4. - The Contractor must provide a privacy awareness communications kit to Contractor resources involved in the SSC Hosted Contact Centre Service that provides an overview on the use of Personal Information.

13. PRIVACY MANAGEMENT PLAN IMPLEMENTATION

13.1. - The Contractor must implement the privacy management plan (all processes, procedures, roles, responsibilities etc), and any subsequent annual updates, within 60 Federal Government Working Days following service acceptance by SSC.

13.2. - The Contractor must provide to SSC within 40 Federal Government Working Days of a request, evidence not older than 12 months (e.g. test results, evaluations, and audits) that the privacy management plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Canada's privacy requirements.

13.3. - If the Contractor determines that it will take more than 40 Federal Government Working Days to provide the requested evidence for the privacy management plan, the Contractor must notify SSC within five (5) Federal Government Working Days of the original request for evidence, and request an extension, in writing with appropriate justification. Granting an extension is within SSC's sole discretion.

13.4. - If changes to the SSC Hosted Contact Centre Service are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by SSC, the Contractor must provide SSC with sufficient detail to support an update to the privacy impact assessment, and obtain approval from SSC for the anticipated change.

13.5. - Within 40 Federal Government Working Days of the Contract being awarded, the Contractor agrees to provide one-page awareness training package instructing its employees and consultants regarding the use of the Personal Information provided by Canada about the Users.

14. INVESTIGATION OF COMPLAINTS AND ACCESS TO INFORMATION

14.1. - The Contractor must exercise, during the term of the contract, processes and controls that preserve the integrity, privacy and accuracy of all information and data and metadata, irrespective of format and in their possession or under their care or control which information and data is generated by, acquired pursuant to or in any other way arises out of their responsibilities and obligations under the contract in order to ensure that the information and data can be used as persuasive evidence in a court of law.

14.2. - The Contractor must, to the extent it is permitted by law, fully cooperate with Canada and assist Canada in the investigation of complaints, regulatory or criminal investigations and prosecutions both regulatory and criminal and access to information requests that includes allowing security audits/inspections and furnishing requested information (e.g. documentation, data protection description, data architecture and security descriptions) as may be required by Canada within five (5) Federal Government Working Days of a request by Canada.

15. INTERPRETATION

15.1. In the case of disputes regarding interpretation of statement of this SOW or any of the terminology contained herein, the ruling of the TA shall prevail.