ANNEX A

FULL PACKET CAPTURE AND SECURITY ANALYSIS TOOL STATEMENT OF WORK

1. INTRODUCTION

1.1. The Security Operations organization of Shared Services Canada (SSC) is responsible for supporting the Information Technology (IT) security systems functions of the Government of Canada (GC). Included in this purview of responsibilities are the integration, engineering, delivery and support of security systems situated within all the member departments of SSC. Both legacy systems and end-state systems are supported in parallel; however, as part of the SSC initiative, these systems will gradually shift to a consolidated, Government wide adoption.

1.2. SSC Security Operations Centre (SOC) has a requirement to replace an end-of-life and end-of-support full packet capture and security analysis solution. This is a critical detection tool that is used on a daily basis by the SSC SOC in order to detect and confirm threats.

2. TERMINOLOGY

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

GC	Government of Canada
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
NCR	National Capital Region
OEM	Original Equipment Manufacturer
RFP	Request for Proposal
SOC	Security Operations Centre
SOW	Statement of Work
SSC	Shared Services Canada
TA	Technical Authority

Note: One (1) gigabit = 0.125 gigabytes or 125 megabytes.

3. BACKGROUND

3.1. The Security Operations team is part of SSC and has a mandate to perform in-service support for several enterprise class security systems applications, including the backend management systems of these applications. Currently, these applications reside within more than 43 department networks. However, as part of the SSC initiative, these systems will gradually shift to a consolidated, Government wide adoption.

3.2. The primary purpose of this Request for Proposal (RFP) is to replace an end-of-life and end-of-support (as of March 31, 2016) full packet capture and security analysis solution. The entire solution requires replacement. The core of the contract consists of the goods and services required to address this requirement.

3.3. The second objective of the RFP is to establish a method to expand the solution over time and expand within the GC over time. Full packet capture and security analysis tools are used in a limited fashion within the GC; this RFP is one of the methods being used to standardise on a common tool across SSC operated networks.

3.4. This RFP is not for a generic network monitoring tool set. Rather, its primary purpose is for packet capture in the context of security analyses. The end-users of the solution will be the SOC. SOC operators will use the tool to confirm third party Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts, to replay suspected attacks, and as part of security investigations.

4. OBJECTIVE

4.1. The core objective of the contract is to replace an end-of-support full packet and security analysis tool by no later than March 31, 2016. The replacement effort will require both goods and services as follows:

4.1.1. Hardware and software required to capture, store and analyze traffic from network links that are used to connect a SSC partner to the Internet, via an existing network tap supplied by the Crown, and perform complex security analysis on the captured traffic.

4.1.2. Hardware and software required to manage all appliances in a centralized manner.

4.1.3. Vendor provided (or vendor partner provided) short term professional services package that will be used to assist SSC in deploying the solution efficiently.

4.1.4. Vendor provided five (5) -day training package for SSC employees on administering the solution.

4.2. The secondary objective is to establish contract options that can be used by SSC to purchase additional goods and services in order to expand the solution over the next three (3) years.

4.3. The RFP will result in four (4) categories of solutions:

4.3.1. Enterprise Solution. Used for larger (2 gigabits per second of average data throughput) SSC networks. This solution will be part of the core of the Contract (two units)

4.3.2. ISP Solution. Used for Government of Canada shared infrastructure, such as the future Government-wide Internet connections. (8 gigabits per second of average data throughput.)

4.3.3. Medium solution. (1gigabit per second of average data throughput)

4.3.4. Virtual, used for smaller capacity partner requirements.

4.4. All categories of solutions must have a retention target of 14 to 30 days of captured traffic. Vendors must size storage to meet these requirements.

4.5. All categories of solutions must have a retention target of 30 to 90 days of metadata. Vendors must size storage to meet these requirements.

4.6. Solution may be deployed in a fully closed network with no Internet access.

4.7. The end-state of the solution is to scale across the Government of Canada. This end state consists of a Central Management solution located in a Federal SOC. The central system would connect to the remote sensors via a national security management network. Figure 1 shows a high level diagram of the use case:

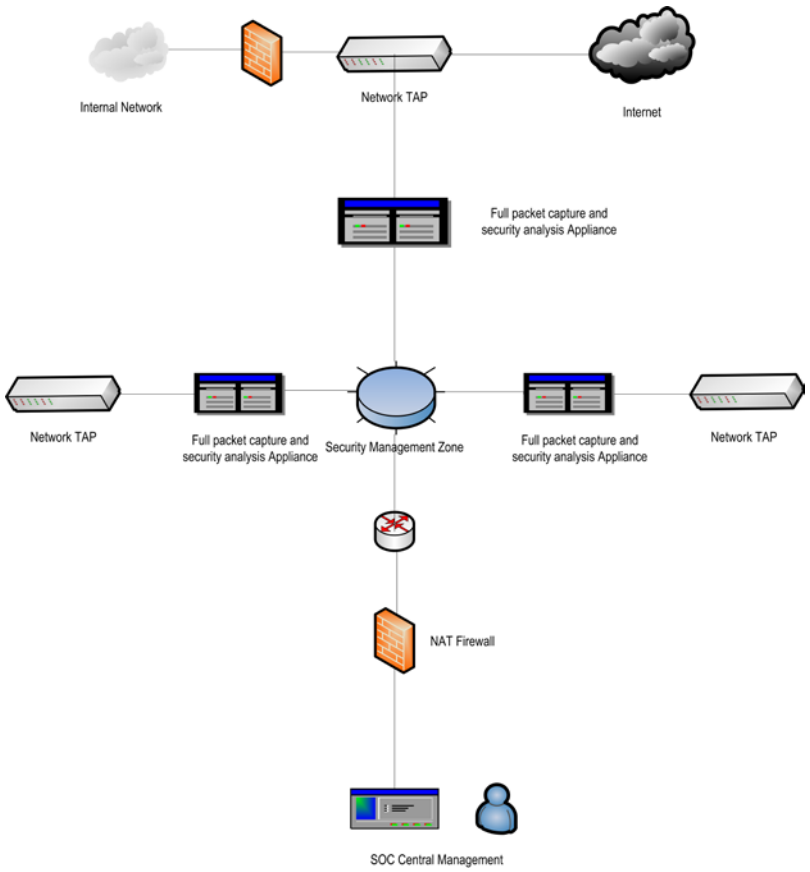

Figure 1. Use Case

5. SCOPE OF WORK

5.1. The core of the contract comprises:

5.1.1. Two (2) Enterprise capacity hardware solutions and first year of maintenance and support. A solution can consist of a single appliance or multiple appliances, as long as they meet all mandatory requirements and the rated points as disclosed in this SOW. Each solution will receive tapped network flows from an existing network tap switch supplied by the Crown. The traffic flow throughput is expected to range between 2 gigabits per second to 10 gigabits per second (as a burst).

5.1.2. One (1) central management system that can be used to manage all appliances, and first year of maintenance and support. A solution can consist of a single appliance or multiple appliances, as long as they meet all mandatory requirements and the rated points as disclosed in this SOW. The central management system will be used to upgrade appliances, and provide a consolidated view into the analyses of captured traffic by the appliances.

5.1.3. On site instructor led training held within the City of Ottawa, Ontario, consisting of 35 to 40 hours over five (5) consecutive business days.

5.1.4. Ten (10) days of professional services in order to help deploy the core solution efficiently, including:

- Engineering
- Testing
- Optimization
- System configuration

5.2. The optional component of the contract includes:

5.2.1. Option to purchase maintenance and support for year 2 and 3 of the equipment purchased as part of the core contract requirement (two Enterprise packet capture appliances, and one central manager).

5.2.2. Option to purchase additional Enterprise capacity hardware solutions for up to three (3) years at the original bid price.

5.2.3. Option to purchase ISP capacity hardware solution for up to three (3) years at the price set by bid.

5.2.4. Option to purchase "medium" capacity hardware solution for up to three (3) years at the price set by bid.

5.2.5. Option to purchase virtual capacity solution for up to three (3) years at the price set by bid.

5.2.6. Option to buy additional five (5) day training package(s) for up to three (3) years at the price set by bid.

5.2.7. Option to buy an additional ten (10) days of professional services deployment package for up to three (3) years at the price set by bid.

5.2.8. Option to purchase any modules, features, or enhancements that can be activated on the solution that are outside the scope of the core requirements.

6. DELIVERABLES

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

6.1.1. All hardware and software included in the Enterprise, ISP, medium, and virtual packet capture and security analysis solution. This includes 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.

6.1.2. If applicable, the subscription of the first 12 months of the Network Threat Intelligence service

6.1.3. All hardware and software included in the central management system. This includes 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.

6.1.4. Five (5) days of training including:

- Classroom facilities suitable to accommodate ten (10) students must be provided by vendor.
- An Original Equipment Manufacturer (OEM) approved instructor to be on site to teach the class.
- All classroom material including workstations to complete labs.

6.1.5. Ten (10) day professional services package including:

- System and build documentation as required in hard copy and electronic copy.
- Project documentation as required.
- Source code, including coding comments, of any customized scripts required to implement the solution.
- Knowledge transfer to designated Crown resource(s) as required.

7. ON-SITE PROFESSIONAL SERVICES RELATED GOODS

7.1. Location of Work

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.

7.2. Work Guidance

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

7.3. Status Reports

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

7.4. Support Resources

The resource will be provided with office resources.

7.5. Security Clearance

The professional services resource for the ten (10) day installations must have a Level 2 - Secret clearance. Bidder must specify security clearance file number and expiration date.

7.6. Normal Working Hours

Normal working hours will be no earlier than 7:00 am to no later than 6:00 pm EST Monday through Friday. For the ten (10) day professional service package, 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.

7.7. Language Requirements

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

8. TRAINING SERVICES RELATED GOODS

8.1. Location of Work

The training resources must be available to work at GC facilities located within the National Capital Region (NCR).

8.2. Work Guidance

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

8.3. Support Resources

The resource will be provided with office resources, but is required to provide a computing device.

8.4. Security Clearance

The resource for the training is not required to have a Government of Canada security clearance.

8.5. Normal Working Hours

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

8.6. Language Requirements

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

9. PROPRIETARY INFORMATION

9.1. Non-Disclosure

9.1.1. 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.

9.1.2. 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.

10. INTERPRETATION

10.1. 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.