REQUEST FOR PROPOSAL NO 232

SECURITY INFORMATION AND EVENT MANGEMENT (SIEM)

This is a Request for Proposal ("RFP") to acquire a Security Information & Event Management (SIEM) solution that can be integrated with the Office of the Auditor General of Canada's (OAG) current network infrastructure. The RFP provides proponents with the relevant operational, performance, application, and architectural requirements of the system. The OAG **is not interested** in acquiring managed services and/or a hosted solution.

This procurement has been set aside under the federal government's Procurement Strategy for Aboriginal Business (PSAB). In order to be considered, a supplier must certify that it qualifies as an Aboriginal business as defined under PSAB and that it will comply with all requirements of PSAB.

This procurement is set aside from the international trade agreements under the provision each has for set-asides for small and minority businesses. Further to Article 1802 of the Agreement on Internal Trade (AIT), AIT does not apply to this procurement.

The OAG will consider entering into a contract with the proponent that provides the proposal rated as best value as determined using the evaluation criteria described in Section 4, "Basis and Method of Evaluation".

This Request for Proposal, in addition to this covering note, consists of the following:

1 RFP GENERAL INSTRUCTIONS AND CONDITIONS 3

1.1 FORMAT OF PROPOSAL 3
1.2 ENQUIRIES 4
1.3 DEFINITIONS AND ACRONYMS 5

2 STATEMENT OF WORK 6

2.1 BACKGROUND 6
2.2 CURRENT IT ENVIRONMENT 6
2.3 PURPOSE 7
2.4 DESCRIPTION AND SCOPE OF WORK 7
2.5 MANDATORY TECHNICAL REQUIREMENTS 9
2.6 RATED REQUIREMENTS 10
2.7 DELIVERY SCHEDULE 10
2.8 REFERENCES 10

3 PROPOSAL STRUCTURE AND PAGE LIMIT 11

3.1 PRODUCT DESCRIPTION 12
3.2 MANDATORY REQUIREMENTS 12
3.3 RATED REQUIREMENTS 12
3.4 FINANCIAL REQUIREMENTS 13

4 BASIS AND METHOD OF EVALUATION 16

4.1 EVALUATION PROCESS 16
4.2 METHOD OF SELECTION 16
4.3 MANDATORY REQUIREMENTS - CONTRACTING 16
4.4 MANDATORY REQUIREMENTS – TECHNICAL 16
4.5 RATED REQUIREMENTS - TECHNICAL 17
4.6 MINIMUM TECHNICAL SCORES 17
4.7 FINANCIAL EVALUATION 17
4.8 SCORING SYSTEM 17

5 CONTRACT TERMS AND CONDITIONS 20

5.1 SECURITY CLEARANCE 20
5.2 LANGUAGE 20
5.3 PRIORITY OF DOCUMENTS…… ……20
5.4 OTHER CONTRACT CONSIDERATIONS……..……..20

APPENDIX A: DECLARATIONS AND CERTIFICATIONS (MANDATORY)..... 24

A1. PROPONENT'S BUSINESS INFORMATION..... 24
A2. PROPOSAL VALIDITY PERIOD 24
A3. EMPLOYMENT EQUITY..... 24
A4. CERTIFICATION OF EDUCATION AND EXPERIENCE 25
A5. CERTIFICATION OF AVAILABILITY AND STATUS OF PERSONNEL 25
A6. CERTIFICATION OF FORMER PUBLIC SERVANT IN RECEIPT OF A PENSION..... 25
A7. CERT. FOR THE SET ASIDE PROGRAM FOR ABORIGINAL BUSINESS 27

APPENDIX B: MANDATORY REQUIREMENTS CHECKLIST—CONTRACTING..... 29

APPENDIX C: EVALUATION CRITERIA AND SCORING GRID 30

APPENDIX D: PILOT SCENARIOS 44

Should you have any questions, please contact the Paul Fowlow by telephone at 613-952-0213 extension 5215 or by email at paul.fowlow@oag-bvg.gc.ca

SECTION 1

1 RFP GENERAL INSTRUCTIONS AND CONDITIONS

The proposal **MUST** be received at the following address no later than 2:00 p.m., Ottawa time on **March 11, 2014**. Note that proposal packages must be received at the Mail Scanning Room in the CD Howe Building and proponents should make appropriate time allowances for this process.

Office of the OAG of Canada
Contract & Procurement Services
240 Sparks Street—CD Howe Building
Main Scanning Room S-143; S-1 Level
Ottawa, Ontario K1A 0G6

Contracting Authority:
Paul Fowlow
Contract and Procurement Services
Telephone: 613-952-0213 extension 5215
Fax: 613-957-9735
Email: paul.fowlow@oag-bvg.gc.ca; GX-Contracting-Contrats@oag-bvg.gc.ca

1.1 FORMAT OF PROPOSAL

Five (5) copies of the Technical Proposal and two (2) copies of the Financial Proposal should be submitted. The medium for all original proposal data should be 8 ½" x 11" paper, printed double-sided. Fonts used should not be smaller than 11 point with margins of a minimum size of 1 inch top, bottom, left and right.

One (1) additional copy of the Technical Proposal and one (1) additional copy of the Financial Proposal should to be submitted in electronic format. Copy should be in PDF format on an electronic storage medium (e.g., memory stick, CD ROM).

Financial Proposals should be submitted in a **separate**, easily identified envelope. Both the Financial and Technical Proposals shall be submitted together as one package. The outside of the package should clearly identify the name and address of the submitting firm. The package should be clearly labelled **"RFP No. 232 –Security Information and Event Management (SIEM)"**.

Proponents have the sole responsibility for the timely receipt of the proposal by OAG. Late proposals will be returned unopened. Proponents shall prepare a proposal addressing all the requirements as stated within this RFP.

As part of Appendix A of their proposal, Proponents **MUST** certify the following:

a. Proponent's Procurement Business Number (PBN) and/or GST/HST number;

b. Legal name of Proponent, company address, telephone and fax number;

c. Point of contact for proposal: the name of the point of contact, telephone, fax number and email address.

d. Confirmation that the proposal submitted in response to this RFP is valid in all respects, including price, for a period of not less than one hundred and twenty (120) days from the closing date of the RFP.

Proposals **MUST** be organized as prescribed, and use the proposed numbering scheme, as described in Section 3.

Electronic transmission of proposals by such means as electronic mail or facsimile **will not** be accepted.

The OAG may cancel the proposal call at any time without further obligation to the proponents.

The OAG may ask Proponents to substantiate any claims made in their proposals.

If a Proponent feels that the requirements stipulated are unnecessarily restrictive in any way and wishes to deviate from the requirements, the Proponent must give a detailed explanation as to why such a deviation is being proposed. The OAG is not obligated to accept any proposed deviations.

The cost of preparing a proposal will not be reimbursed by the OAG.

Any amendment by the OAG to this RFP shall be in writing.

The use of Internet-links to answer RFP questions is prohibited. Links to websites and other Internet information will not be reviewed and hence not be evaluated by the OAG.

Proposals will be evaluated as described in Section 4. The proponent **MUST** comply with the mandatory and rated requirements. Failure to comply with **ANY** mandatory requirement will render the proposal non-compliant and it will receive no further consideration.

The requirements of the Federal Proponent's Program for Employment Equity may apply to this RFP (refer to Appendix A of this RFP).

Proposals received in response to this request shall become the property of the OAG and will not be returned.

1.2 ENQUIRIES

All enquiries concerning this procurement should be submitted in writing by facsimile or electronic mail to the OAG Contracting Authority identified previously (Section 1).

Enquiries should be received by the OAG Contracting Authority no less than five (5) working days prior to the bid closing date (per section 1 above) to ensure sufficient time to provide a response. The OAG may not reply to any enquiries received after that time.

Proponents should reference as accurately as possible the numbered item or section of the RFP to which the question applies. Care should be taken by Proponents to explain each question in sufficient detail in order to enable the OAG to provide an accurate answer.

To ensure consistency and quality of information provided to Proponents, the Contracting Authority will simultaneously provide to all Proponents any information with respect to significant enquiries received and the replies to such enquiries without revealing the sources of the enquiries.

All enquiries and other communications with OAG officials pertinent to this RFP throughout the solicitation period are to be directed **ONLY** to the Contracting Authority named herein (per Section 1). Noncompliance with this condition during the bid solicitation period may, for that reason alone, result in disqualification of a Proponent's proposal.

Should sufficient questions be raised, a Proponent's conference may be held on OAG premises. Should a Proponent's conference be held, notification will be provided to all Proponents of the date, time and location of the conference.

This RFP constitutes the entire understanding of the work required; in the event of any differences between the RFP and Proponent submitted documents, the RFP will govern. Submitting a bid with terms and conditions that differ from the terms and conditions set out in this RFP may cause the OAG to consider the bid non-responsive.

After the Successful Proponent is selected, and has conducted a successful pilot, a contract will be entered into (issued) based on the services described in this RFP.

1.3 DEFINITIONS AND ACRONYMS

1.3.1 DEFINITIONS

Definitions are capitalized throughout and are for the purposes of this document and RFP process only and not for any other purpose.

“Equipment” means all hardware, firmware and/or software necessary to Implement the SIEM.

“Implement”/“Implementation”/“Implemented” means design, manage project, pilot, document, install, configure, program, test, certify and/or commission or any other activity to ensure the delivery of item in question is fully functional to the OAG’s satisfaction and industry standards. The cost of all Implementation activities is the responsibility of the Successful Proponent.

“include” /“includes”/“including” means “include without limitation”, “includes without limitation” and “including without limitation”, respectively, and the words following “include”, “includes” or “including” will not be considered to set forth an exhaustive list.

“Proponent” means an individual, a corporation, proponent, joint venture, association, pension fund or a consortium of any of the foregoing that may submit or that has submitted a Proposal.

"Services" means the services required to Implement the Equipment for the SIEM.

“Solution” means all of the Equipment, Software and Services required that makes up a Proponent’s proposal

“Successful Proponent” means the Proponent who has been selected by the OAG and to whom a contract is expected to be awarded, pending the successful pilot.

“SIEM” is comprised of, but not limited to, the Equipment and Services necessary to Implement the SIEM Project as prescribed by the requirements of this RFP.

“Contractor” means an individual, a corporation, proponent, joint venture, association, pension fund or a consortium to whom a contract has been issued.

1.3.2 Acronyms

“GUI” means Graphical User Interface

“IP” means internet protocol

“NTP” means Network Time Protocol

“OAG” means the Office of the Auditor General of Canada.

“SOC” means Security Operations Center.

“TCO” means the Total Cost of Ownership.

“**SOW”** means Statement of Work

“RFP” means Request for Proposal

‘POE” means Power over Ethernet

“AD” means Microsoft’s Active Directory

“SIEM” means Security Information and Event Management

SECTION 2

2 STATEMENT OF WORK

2.1 BACKGROUND

The Office of the Auditor General of Canada (OAG) is an independent and reliable source of the objective, fact-based information that the Parliament of Canada needs to fulfill one of its most important roles: holding the federal government accountable for its stewardship of public funds. The OAG audits departments and agencies, most Crown Corporations, and many other federal organizations; it is also the auditor for the governments of Nunavut, the Yukon, and the Northwest Territories. The OAG has approximately 530 staff in Ottawa and 90 staff in regional offices, located in Vancouver, Edmonton, Montreal and Halifax.

The OAG is organized into one (1) Executive Office, ten (10) audit groups, one (1) Professional Practices group and one (1) audit services group (i.e. Finance, HR, IT). The standard office hours are Monday to Friday, 7AM to 6PM – except federal holidays. The OAG expects little to no organizational growth over the next few years. The OAG has a standard set of telephony and telephony-related requirements to drive their business.

The OAG audits federal government operations and provides Parliament with independent information, advice, and assurance regarding the federal government's stewardship of public funds. We conduct performance audits of federal departments and agencies, annual financial audits of the government's financial statements, and special examinations and annual financial audits of Crown corporations. Since 1995, the OAG has also had a specific environmental and sustainable development mandate, established through amendments to the Auditor General Act. Our audit findings—which include good practices, areas requiring attention, and recommendations for improvement—are reported to Parliament.

2.2 CURRENT IT ENVIRONMENT

The OAG Local Area Network is composed at its edge of HP ProCurve 2910 al switches without PoE that service about 530 clients in the Ottawa 240 Sparks office and 90 clients in four regional offices (Montreal, Halifax, Edmonton, and Vancouver).

The OAG's corporate applications are located and managed centrally from the Ottawa Office and serve the Regions through dedicated high-speed wide area network links between the Regional Offices. All Internet connection requests from the Regional Offices are channelled through our InterGov connections to Ottawa and then to the Internet. All connections between the Main Office, the Regional Offices and the Internet are done through the Government of Canada SCNet. The bandwidth access is as follows:

- Ottawa Main Office (530 + connections)
  - 20 Mbps connection to the Internet
  - 40 Mbps connection to InterGov
- Disaster Recovery Site
  - 20 Mbps connection to the Internet
  - 30 Mbps connection to InterGov
- Halifax
  - 10 Mbps connection to InterGov

- Montreal
  - 10 Mbps connection to InterGov
- Edmonton
  - 10 Mbps connection to InterGov
- Vancouver
  - 10 Mbps connection to InterGov

The OAG's client base is Windows 7 (64-bit) and the office suite is Microsoft Office 2010. We run Microsoft Lync 2010 as our unified messaging product of choice and all OAG internal users authenticate to the network through Microsoft Active Directory (AD). All clients' PC/Laptops run anti-virus/end-point security.

The server infrastructure consists of mostly Microsoft Windows Server 2008 R2 (~140), virtualized at about 80% with VMWare 5.0. The OAG has a disaster recovery site that hosts a subset of the environment in case of disaster. In addition, the OAG's server infrastructure consists of:

- **Web Services/Applications**: Web services, IIS, .Net Framework, Microsoft – business software & office products, Microsoft Exchange.
- **Other servers/OS**: Red Hat Linux (3), HP UNIX (3), Oracle Linux (2), external DNS Servers (2), VMWare ESXi (9)
- **Databases**: Oracle and MS SQLServer
- **Other components**: WiFi AP (~60), Polycoms endpoints (~10 including bridge and cma)

2.3 PURPOSE

The OAG is currently revamping its network infrastructure. Consequently, the OAG intends to invest in tools that provide for better intelligence and more proactive security controls. The purpose of this RFP is to select a competent Proponent who has sufficient experience supplying, installing, training and supporting industry leading SIEM solutions. The selected SIEM solution will allow the consolidation of system logs that are a part of the OAG's critical infrastructure and allow the ability to alert the organization to ongoing issues and to track incidents back to an original event. The purpose of this RFP is to acquire hardware, software, maintenance support and Implementation services. The OAG is **not interested** in acquiring managed services and/or a hosted solution.

This document describes the SIEM project with a detailed scope outlined in Section 3 and mandatory requirements in Section 4. All Proponents must respond to the mandatory and rated requirements as outlined in this RFP to ensure their proposal is deemed compliant. However, Proponents are encouraged to provide alternate solutions that meet the intent of requirements where better value or increased operational effectiveness can be realized.

Any resulting contract from this RFP for hardware, software and maintenance services is expected to be valid for 3 years. The Total Cost of Ownership (TCO) over the first three (3) years **shall not exceed** the budget of $100,000.00 CDN (including HST or any other applicable taxes). The OAG may disqualify any proposals that exceed this budget. The OAG reserves the right to purchase maintenance support for up to two (2) additional two (2) year periods.

2.4 DESCRIPTION AND SCOPE OF WORK

The SIEM Project includes all of the Equipment and Implementation services necessary to provide a SIEM Solution to connect to the various network elements and meet the capacity, functionality and feature requirements outlined in this RFP. The scope of this RFP includes the following:

i. Identification and recommendation of an appropriate SIEM solution, which fits the OAG's requirements and allows for future growth;

ii. Supply, configuration, installation and testing of the proposed solution, including any required interfaces and data conversions;

iii. Provision of initial and extended warranties and technical support services (including detailed initial acquisition costs and on-going support options by year);

iv. On-site hardware installation and setup, software configuration and user settings;

v. Training for hardware, software configuration and SIEM management software;

vi. Provision of documentation in printed and electronic format, including administrative and end user manuals, troubleshooting guides or Q&A.

The OAG expects that the Solution will be functional and be fully integrated into our current architecture once the Proponent completes their work. The Proponent is to provide for sufficient training so that up to six (6) OAG employees will be able to effectively use and maintain the proposed Solution.

2.4.1 Security and Privacy

A *Threat and Risk Assessment (TRA)* and a *Privacy Impact Assessment* (PIA) will be conducted in relation to the winning solution. The OAG reserves the right to validate the compliance with security standards for encryption methodology and secure deployment of the winning solution prior to authorizing payment. The OAG also reserves the right to **reject** the proposed solution or to require correction by the Proponent should any part of the solution provided not be to the OAG's satisfaction. The Proponent shall also assume all costs associated with any correction(s) required by the OAG.

2.4.2 Pilot

In order to ensure that the best possible solution is selected the Successful Proponent is expected to implement the proposed solution for a pilot period of no less than five (5) days. The pilot period will allow the Successful Proponent to prove functionality and integration of the proposed solution with the OAG's IT systems and to "showcase" its capability. The evaluation of the pilot will consist of two (2) phases:

> Phase 1: The proponent will have to prove that their proposed solution meets all of the Mandatory Technical Requirements as stated in their proposal (see Section 2.5).
>
> Phase 2: The proponent is to demonstrate how their proposed solution performs against the scenarios listed in Appendix D. This phase will be used to verify the rated technical requirements; therefore, the OAG evaluation committee **may adjust points awarded** in Step 2 of Section 4.2. The scenarios listed in Appendix D are designed to verify that the solution meets the minimum scores required in TR-05, TR-06, TR-11 and TR-12. If the proponent fails to fully demonstrate that the proposed solution meets all the minimum scores, the Proponent will be declared non-compliant.

The pilot is expected to take place as soon as possible following the selection of the Successful Proponent. The OAG may also contact the supplied references during phase 2 of the pilot.

Should the Successful Proponent fail the pilot, the OAG will ask the proponent with the next highest score to pilot their proposed solution. Only upon the successful completion of pilot, will a contract be issued to the Successful Proponent.

All costs associated with the pilot, including integration of other components, shall be borne by the Proponent.

2.5 MANDATORY TECHNICAL REQUIREMENTS

The proposed SIEM Solution **MUST** possess the following seven (7) technical characteristics at the time of proposal submission. Proponents are to provide in their technical proposals a detailed description of how their product meets each of these characteristics. The OAG will also verify claims through consultations with the supplied references and through the on-site pilot as indicated in Section 2.4.2.

Table 1 – Mandatory Technical Requirements

Identifier	Description
MR-01	All proposed Solutions **MUST** be "Off-the-Shelf", meaning that each Solution is commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any part of the proposed Solution is a fully compatible extension of a field-proven product line, it **MUST** have been publicly announced on or before the date that the proposal is submitted.
MR-02	As part of the proposed solution, if any software and/or middle-tier components need to be deployed on a server and/or virtualized, they **MUST** be able to operate on the OAG standard server platform: • Windows Server 2008 R2 or later on a 64 bit platform. • VMWare v5.0.
MR-03	As part of the proposed solution, if any software **MUST** operate on user's laptop/desktop, the solution **MUST** operate on the following minimum configuration: • Windows 7 (64-bit OS) • Core 2 Duo • 4 GB RAM • 100 GB Hard Drive. Any software solution requiring authentication **MUST** provide for Single-Sign-On (SSO) authentication with Microsoft Active Directory, without the use of an intermediary directory for all users at the OAG. At the OAG we define SSO as follows: a user connects to the OAG network using a supplied username/password. Once logged into the OAG network, a user never has to supply a username or password to access business applications. This must also include the automatic provisioning of users from Microsoft AD without any manual intervention. The OAG prefers that the solution not involve AD schema extension.
MR-04	The proposed solution **MUST** provide a complete backup and restore capability itself, through an integrated database or be integrated through the OAG's backup software: CommVault.
MR-05	Proponents **MUST** provide on-site training for the installation, operation, maintenance and customization of the solution to be provided to up to 6 OAG administration staff members.

MR-06	Technical Support: Proponents **MUST** provide technical support, including issue/problem reporting and assistance with response within 24 hours of an issue being reported. Any costs for support must be included in the costs specified in the cost summary chart in Section 3.4.
MR-07	Experience**:** Proponents **MUST** have at least three (2) years of experience Implementing similar solutions.

2.6 RATED REQUIREMENTS

The Rated Requirements listed in Appendix C shall be completed by all Proponents. The OAG will assess the proposals using the evaluation criteria listed in Appendix C.

2.7 DELIVERY SCHEDULE

The Contractor shall deploy the proposed solution within fifteen (15) business days of contract award. After a successful Proponent is selected, the proposed solution shall be deployed before 31 March 2014.

Training must occur within twenty (20) business days of contract award.

2.8 REFERENCES

As part of their technical proposal, proponents are to provide a list of references of at least one (1), but ideally three (3) locations where their solution is installed and has been operational for at least 3 months. Ideally, references should be for installations comparable in size and business scope as the OAG. Using the chart below please provide up to date contact information for references that can be used to verify the installation of the software and attest to its performance and capabilities.

References may be contacted to help validate proponent claims and to seek feedback on the proponent and the proposed solution's capabilities and shortcomings. References may be contacted during any phase of the evaluation process.

Table 2 - References

REFERENCE	
Company/Organization Name	
Address	
Installation Date (approximate)	
Contact Name & Title	
Contact Co-ordinates (telephone # and email address)	

SECTION 3

3 PROPOSAL STRUCTURE AND PAGE LIMIT

The proponent's proposal **MUST** be organized using the content numbering scheme and is subject to the maximum page limit described below.

The Technical Proposal is limited to a maximum of 60 pages. This includes the sections related to mandatory and rated technical requirements but excludes the Appendices. Any information provided in excess of the stipulated maximum within the core body of the Technical Proposal will not be taken into account in the evaluation of the proposal. Title pages, table of contents, and tabbed dividers are not included in this limit, and therefore must not include material intended for evaluation.

Table 3 – Proposal Structure

Required Structure of Proposals and Content Numbering

Technical Proposal

1.0 Description of Product Being Proposed

2.0 Response to Mandatory Requirements

2.1 Contracting Requirements – Table from Appendix B

2.2 Technical Requirements – Response to Mandatory Technical Requirements from Section 2.5

3.0 Response to Rated Requirements

3.1 Corporate

3.2 Product Architecture

3.3 Product Features

3.4 Product Operations

3.5 Project Management and Implementation

3.6 Training and Transition Support

3.7 Post Implementation Support and Maintenance

3.8 References

Appendices

A Certifications

B Sample Software License and Maintenance/Support Agreements

C Supplementary Product Information (Optional)

Financial Proposal (under Separate Cover)

Proponents shall conform to the required format proposed below. The original order and identification of the requirements shall be maintained in the RFP Submission. Failure to conform, at the sole discretion of the OAG, may result in the Proponent's proposal being rejected. All Requirements in this RFP have unique identifiers and a description. Proponents are to repeat

each requirement identifier and description and insert the response into the requirements table below each requirement as a new row, as follows:

Table 4 – Requirements Table Model

Requirement Identifier (i.e. TR-XX)	Requirement Description
Response from Proponent to requirement TR-XX	

It is vital that Proponent's proposals provide detailed and comprehensive responses to the requirements in this RFP while at the same time ensuring that responses are precise and to the point. Proponents shall use the document structure defined above for their responses including the financial template, to facilitate equitable evaluation.

Information to be evaluated must be provided within the 60 pages. We encourage Proponents to present their information in portrait format. Material such as corporate literature or website information can be referenced, but merely to supplement the response and not to replace it. Such information will not be rated.

The following provides additional guidance on the required content of the different sections of the proposals.

3.1 PRODUCT DESCRIPTION

Proponents' are to provide a complete description of the Equipment they are proposing to meet the OAG's requirements. This description is to provide specific version numbers, product, part and/or item numbers describing all of the hardware and/or software components that comprise the proposed solution. The description should also briefly describe the capabilities and the function of the hardware and/or software including options, potential additions, etc. Proponents may include brochures, testimonials and other support materials as Appendix C of their proposal.

3.2 MANDATORY REQUIREMENTS

Proponents' proposals **MUST** meet **all** of the RFP mandatory requirements in order for their proposals to be considered for evaluation. Failure on the part of the proponent to meet any one (1) or more of the mandatory requirements will result in their proposal being deemed non-compliant and given no further consideration.

There are two types of mandatory requirements: Contracting Mandatory Requirements and Technical Mandatory Requirements.

Contracting Mandatory Requirements are indicated in Section 4.3 and Appendix B. Proponents **MUST** complete the table in Section 4.3 and include it as part of the technical proposal. In the table, proponents are to indicate beside each of the requirements the relevant page number(s) from their proposal where the requirements are addressed (Mandatory Item M-5).

Technical Mandatory Requirements are indicated in Section 2.5. In their technical proposals, proponents are to provide a brief description of how their proposed solution meets each of the mandatory technical requirements.

3.3 RATED REQUIREMENTS

Technical Proposals meeting **all** of the Mandatory Requirements (Contracting & Technical) will have their technical proposal evaluated by the evaluation committee.

In their technical proposals, proponents are to clearly describe how their proposed SIEM Solution meets each of the rated technical requirements.

As indicated in Section 2.4.2, the OAG will assess the Successful Proposal through the use of a Pilot.

3.4 FINANCIAL REQUIREMENTS

As indicated in Section 2.3, the OAG expects that the solution acquired as a result of this RFP will be effective for at least three (3) years. The OAG reserves the right to purchase maintenance support for up to two (2) additional two (2) year periods, at the OAG's sole discretion subject to budgetary limitations.

The OAG wishes to understand and evaluate the **full** cost (Total Cost of Ownership) of the proposed software. Therefore, Proponents are to provide a three (3) year cost summary using the following chart. The total cost for the three years of the agreement will be used to evaluate the financial proposals. See below for a description of each cost element.

Table 5 – Three Year Total Cost Summary

Line Item	Description	Year 1 Cost	Year 2 Cost	Year 3 Cost
Equipment – provide the itemized cost for the following:				
1	SIEM and miscellaneous equipment (e.g., software, hardware)	$	$	$
2	Implementation Services	$	$	$
3	Licensing	$	$	$
4	Training (system and user)	$	$	$
5	Transition Support	$	$	$
6	Warranty and maintenance support (hardware and software)	$	$	$
7	Documentation	$	$	$
8	Other costs: (if any, please describe)	$	$	$
Subtotal by Year		$	$	$
GRAND TOTAL[1]		$		

[1] The Total Cost of Ownership (TCO) over the first three (3) years shall not exceed the budget of $100,000.00 CDN (including HST). The OAG may disqualify any proposals that exceed this budget.

The following describes some of the potential cost elements for each line item.

1. SIEM and miscellaneous equipment List and describe here all hardware and software that comprise your solution with itemized costing as appropriate. Also include any miscellaneous equipment that is required to operate the solution.

2. Implementation Services List and describe here all costs associated with the design, the project management, documenting, installation, configuration, programming, testing, certifying and/or commissioning or any other activity required to ensure the proposed solution is fully functional to the OAG's satisfaction and industry standards. This includes:

   a) Installation: Describe any labor, equipment, supplies, or other costs associated with installing, configuring or adapting the proposed software to the OAG IT environment.

   b) Integration: Describe any labor, equipment, supplies, or other costs associated with integrating the proposed software into the OAG's current IT architecture and back-end software.

   c) Project Management: If there are project management fees associated with your proposed software, list and describe them here.

3. Licensing List and describe all licensing, implementation, maintenance, support, and training fees associated with your proposed software. Proponents are also to include any add/remove costs for all license-types.

   As separate items, Proponents are to list and describe any Third-Party Software (Middleware) and their associated cost that would be required to implement or optimally operate the solution. Proponents are also to list and describe any subscription fees, add/remove costs for all such licenses.

4. Training If there are any fees for training of the OAG support personnel (as described in Section 2.4), such fees are to be listed and described here.

5. Transition Support Proponents are to list and describe any costs associated with assisting the OAG with Help Desk readiness and business continuity planning.

6. Warranty and Maintenance Support Proponents are to list and describe any ongoing costs associated with the operation and maintenance of their proposed solution

7. Documentation If there are fees associated with user or technical documentation, Proponents are to list and describe them here.

8. Other Costs Proponents are to list and describe any other costs associated with their proposed solution. Proponents shall include any other costs they consider relevant to the OAG for the successful implementation of the proposed SIEM solution. This can include, but is not limited to, cost to acquire additional storage or backup capacity.

It is not necessary for Proponents to charge or list a cost for each element, only those that apply to their pricing model. If, for example the cost of documentation is included in the price of the software, proponents can indicate that.

As indicated in Section 2.3, the OAG reserves the right to purchase maintenance for the software for up to two (2) additional two year periods. Accordingly, proponents are to provide a cost for each of the option years in the following chart.

Table 6 – Option Year Cost Summary

Costs	Year 4	Year 5	Year 6	Year 7
Maintenance Support				
Other (specify)				

Payment will be made upon delivery and implementation of the solution. For other elements of the Solution, payments will be made upon their satisfactory delivery. For example, payment of any training costs will only be payable upon the successful training of OAG staff. Maintenance and support will be paid on a yearly basis.

SECTION 4

4 BASIS AND METHOD OF EVALUATION

4.1 EVALUATION PROCESS

An evaluation team composed of OAG officials will evaluate the proposals. The OAG will use a step-by-step approach to selecting the successful proponent. The approach will consist of the steps described in Section 4.2 below. Only proposals that meet the requirements of a particular stage will progress to the following stage(s).

Failure of a proposal to provide information in sufficient detail and depth to permit evaluation against the criteria may render a proposal non-responsive. Proponents are advised that only listing capabilities without providing any supporting explanation or description about the capability will not be considered to be “demonstrated” for the purposes of the evaluation.

4.2 METHOD OF SELECTION

Step 1: The evaluation team will confirm compliance with all mandatory requirements identified in Sections 2.5 and Appendix B. See Sections 4.3 and 4.4 below.

Step 2: Proposals deemed compliant in Step 1 will then be evaluated by the technical evaluation committee as per the rated requirements CR-01 to CR-04 and TR-01 to TR-25, using the criteria and point structure described in Appendix C.

Step 3: Those technical proposals deemed compliant in Steps 1 and 2 will have their financial proposals evaluated by the OAG Contracting Group following the process described in Section 4.7.

Step 4: The highest scoring solution after Step 3 will be deemed to be the Successful Proponent. At this point and as per Section 2.4.5, the Successful Proponent shall be invited to pilot their proposed solution for a period of no less than five (5) days to prove functionality and integration with the OAG’s IT systems. During the pilot period, the proposed solution will be evaluated against the scenarios in Appendix D.

4.3 MANDATORY REQUIREMENTS - CONTRACTING

Proponents **MUST** complete the table in Appendix B and provide it as part of their technical proposal. Proponents are to indicate beside each of the requirements the relevant page number(s) from their proposal where they are addressed (see MC-4).

4.4 MANDATORY REQUIREMENTS – TECHNICAL

The proposed solution **MUST** possess the characteristics described in Section 2.5 at time of proposal submission. As indicated in Sections 2.5 and 3.2, proponents are to provide in their technical proposals a brief description of how their solution meets each of the seven (7) mandatory technical requirements. The OAG will verify claims through the pilot and through consultations with the supplied references.

It is vital that Proponent’s proposals provide detailed and comprehensive responses to the requirements in this RFP while at the same time ensuring that responses are precise and to the point. In order to have their proposals evaluated, Proponents **MUST** adhere to the document structure defined in Section 3 for their responses including the financial template.

Responses shall not make references to corporate literature or website information and any literature that is provided shall exist merely to supplement the response and not to replace it.

For the SIEM, the Proponent must respond to the requirements by providing the solution, which the Proponent will implement, rather than against what could be implemented but hasn't been included in the solution. By virtue of submitting a proposal, Proponents are contractually bound to be able to deliver the solution contained in their proposal.

4.5 RATED REQUIREMENTS - TECHNICAL

Proposals meeting **all** of the Mandatory Requirements will be evaluated and rated using the categories of requirements described in Appendix C using the criteria described therein.

Unless otherwise indicated, the evaluation team will use the following scoring system for each requirement:

Excellent Response = 100% of available points
Very Good = 80% of available points
Good = 60% of available points
Average = 40% of available points
Fair = 20% of available points
Poor or No Response = 0% of available points

The score for each rated requirement is determined by the percentage score assigned multiplied by the weight assigned for each requirement. The sum of the scores for each requirement provides the score for each category.

To confirm findings, the rated requirements will be re-rated during the pilot (using the same evaluation criteria and scoring template described in Appendix C).

4.6 MINIMUM TECHNICAL SCORES

Proponents must receive a minimum score against four of the rated technical requirements (TR-05, TR-06, TR-11 and TR-12) to be considered compliant. See the scoring table matrix in Section 4.8 and Appendix C for the minimum scores.

4.7 FINANCIAL EVALUATION

Those proposals that have met all of the Mandatory Requirements and met or exceeded the minimum technical scores will have their Financial Proposal evaluated by the OAG Contracting Group.

The total cost for the first three (3) years of the agreement will be used to evaluate the financial proposals. Full points (540/540) will be awarded to the proposal with the lowest combined cost. Fewer points will be awarded to all other qualifying proposals based on the percentage differential between their combined cost and that of the proposal with the lowest combined cost; using the following formula:

$$\frac{\text{Lowest Combined Cost (\$)}}{\text{Proponent's Combined Cost (\$)}} \times 540 = \text{Points for Proponent's Financial Proposal}$$

4.8 SCORING SYSTEM

The scoring table below summarizes the points available for each of the rated requirements. It also identifies the applicable minimum point requirements.

Table 7 – Scoring System

Rated Requirements	Maximum Score	Minimum Points Required
Corporate Requirements		
CR-01 - Escalation Process	**25**	**NA**
CR-02 - Quality System	**25**	**NA**
CR-03 - Proponent's Financial Stability, Experience and Support Capabilities	**125**	**NA**
CR-04 - Reference Sites	**100**	**NA**
Technical requirements		
TR-01 to TR-06 - Product Architecture	**330**	**80**[2]
TR-07 to TR-10 - Product Features	**170**	**NA**
TR-11 to TR-15 - Product Operations	**295**	**115**[3]
TR-16 to TR-19 - Project Management and Implementation	**70**	**NA**
TR-20 to TR-21 - Training and Transition	**65**	**NA**
TR-22 to TR-25 - Post Implementation Support and Maintenance	**50**	**NA**
Total Technical Score	**1255**	**NA**
Financial Score	**540**	**NA**
OVERALL TOTAL SCORE (technical + financial)	**1795**	**NA**

[2] TR-05 and TR-06

[3] TR-11 and TR-12

The Proponent with the proposal receiving the highest overall score (Technical + Financial) will be deemed to represent best value to the OAG, and will be declared the Successful Proponent. The Successful Proponent will be invited to pilot their solution.

In the event that two or more proposals receive the same overall score, the proposal with the lowest total cost will be deemed to represent best value to the OAG, and will be declared the Successful Proponent.

SECTION 5

5 CONTRACT TERMS AND CONDITIONS

The contract issued as a result of this RFP will include the following key terms and conditions.

5.1 SECURITY CLEARANCE

All Contractor personnel accessing OAG networks and/or accessing OAG physical office space **must** possess a valid Government of Canada Security Clearance at a minimum level of **Reliability** status. **Clearance must be in place prior to accessing OAG premises and systems**. Contractors will be expected to understand and adhere to the OAG Code of Professional Conduct and the OAG Security Policy. Contractors will sign an undertaking of non-disclosure of information that will require, among other things; that all files and other OAG information are to remain the property of the OAG; that no copies or transcripts of any kind will be made of this information, and that information obtained during the course of the engagement will not otherwise be disclosed. It may be necessary to restrict contractor access to particularly sensitive information.

The OAG will confirm and/or arrange for the security clearance of contractor personnel as required prior to contract award.

5.2 LANGUAGE

The OAG is under the obligation to respect the spirit and letter of the *Official Languages Act*.

5.3 PRIORITY OF DOCUMENTS

The documents specified below form part of and will be incorporated into the resulting contract. If there is a discrepancy between the wording of one document and the wording of any other document which appears on the list, the wording of the document which first appears on the list shall prevail over the wording of any document which subsequently appears on the list:

I. The contract document;

II. This Request for Proposal;

III. The proponent's proposal;

5.4 OTHER CONTRACT CONSIDERATIONS

i. a) Total payments under this agreement will not exceed the contract value, exclusive of the Applicable Taxes on the supply of services. Payment by the Auditor General shall be made within thirty (30) days of the date the Contractor's invoice is received.

b) The Contractor will render accounts on a monthly basis during the term of this agreement showing separately, hours worked, periods and cost of travel and living expenses. For administrative purposes the Auditor General requires the Contractor to advise on a weekly basis hours worked.

c) At any time during the contract period, the parties may agree that the services to be provided or the work to be carried out have been or will be substantially or entirely performed for an amount less than the agreement limit. In such a case, the Auditor General may inform the Contractor of its intention to amend the agreement to reduce the maximum amount of the agreement limit.

d) The Auditor General shall provide at least 14 days' notice of its intention to reduce the maximum amount of the agreement limit and upon the expiry of the 14 day period the parties agree that the amended amount is the maximum amount of the agreement limit. The Contractor will be entitled to claim for services provided up to the amended maximum amount of the agreement limit.

ii. The Auditor General will pay to the Contractor the Applicable Taxes on the supply of services. The Contractor will remit to the Receiver General, in accordance with the provisions of the Excise Tax Act, the Applicable Taxes received in respect of the supply of services under this agreement.

iii. This agreement may be terminated:

a) If the Contractor dies or becomes incapacitated;

b) By either party hereto upon 30 days' notice of termination in writing; or

c) Forthwith by the Auditor General by notice in writing if, in its sole and unfettered discretion, determines that the services of the Contractor hereunder are not satisfactory.

iv. In the event that the assigned individual(s) is unable to complete the work to the satisfaction of the Auditor General, the Contractor will provide, subject to the concurrence of the Auditor General, an alternate with the requisite expertise to complete the assignment.

v. This agreement is a contract for the performance of a service, and the Contractor is engaged under the contract as an independent Contractor for the sole purpose of providing a service. Neither the Contractor nor the Contractor's personnel, if applicable, is engaged by the contract as an employee, servant or agent of Her Majesty. The Contractor agrees to be solely responsible for any and all payments and/or deductions required to be made, including those required for Canada or Quebec Pension Plans, Employment Insurance, Workers' Compensation, or Income Tax.

vi. The Contractor shall treat all information that comes to his/her attention by virtue of carrying out the work under this agreement as privileged and confidential and will not disclose it to any third party either during the course of or after termination of this agreement except as may be necessary to perform the duties hereunder.

vii. The Contractor agrees that all documents, reports, papers or other matters produced by the Contractor pursuant to the services provided or to be provided hereunder shall be the sole and exclusive property of Her Majesty and shall not be disclosed for any purpose to any third party without the prior written permission of the Auditor General or delegate.

viii. The Contractor agrees to abide by the laws of Canada, including laws relating to copyright and specifically agrees not to transfer or copy by any electronic or other means any software owned by or licensed to the Office of the Auditor General. The Contractor also agrees that such software is only to be used for the purposes of work carried out on behalf of the Office of the Auditor General and for no other purpose.

ix. The Contractor declares that, on or before entering into the contract, he/she has not, directly or indirectly, paid or agreed to pay and will not, directly or indirectly, pay a contingency fee to any individual for the solicitation, negotiation or to obtain the contract if the payment of the fee requires the individual to file a return under section 5 of the Lobbyists Registration Act.

x. The Contractor declares that, on or before entering into the contract, he/she has not been convicted of an offence, other than an offence for which a pardon has been granted, under section 121, 124 or 418 of the Criminal Code.

xi. The Contractor consents, in the case of a contract with a value in excess of $10,000 (including taxes), to the public disclosure of basic information, other than information described in any of paragraphs 20(1) (a) to (d) of the Access to Information Act, relating to the contract.

xii. If the Contractor consents, in the case of a contract with a value in excess of $10,000 (including taxes) to the public disclosure of basic information with respect to being a former public servant in receipt of a pension under the Public Service Superannuation Act, in accordance with the Guidelines on the Proactive Disclosure of Contracts.

xiii. If the Contractor makes a false declaration under paragraphs (ix) or (x) or fails to comply with the terms set out in paragraphs (xi) or (xii), the Contractor agrees to immediately return any advance payments and the contracting authority may terminate the contract.

xiv. The Contractor agrees that his/her activities in any workplace of the Auditor General shall not endanger the health and safety of employees of the Auditor General.

xv. No Member of the House of Commons shall be admitted to any part of this agreement or to any benefit arising therefrom.

xvi. The Contractor acknowledges having received and read the “Code of Values, Ethics & Professional Conduct for the Office of the Auditor General of Canada” and agrees to be bound to its terms. In accordance with the Code, the Contractor agrees that he/she has discussed with the Office all actual and potential conflicts of interest that may affect his/her work with the Office.

xvii. The Contractor shall not assign the benefit or burden of this agreement to any other person, firm or company.

xviii. This agreement shall for all purposes be governed by and construed in accordance with the laws of the Province of Ontario.

xix. In accordance with the Financial Administration Act, payment under the contract is subject to an appropriation for the particular service for the fiscal year in which any commitment hereunder would come in course of payment.

xx. The parties understand that the Procurement Ombudsman appointed pursuant to Subsection 22.1(1) of the Department of Public Works and Government Services Act will:

a) On request, and consent of the parties, participate in an alternative dispute resolution process to resolve any dispute between the parties respecting the interpretation or application of a term and condition of this contract and their consent to bear the cost of such process, provide to the parties a proposal for an alternative dispute resolution process to resolve their dispute.

b) Review a complaint filed by the Contractor respecting administration of this contract if the requirements of Subsection 22.2(1) of the Department of Public Works and Government Services Act and Sections 15 and 16 of the Procurement Ombudsman Regulations have been met, and the interpretation and application of the terms and conditions and the scope of the work of this contract are not in dispute.

The Office of the Procurement Ombudsman may be contacted by telephone at 1-866-734-5169 or by e-mail at boa-opo@boa-opo.gc.ca

xxi. The Contractor shall provide all manufacturers' terms and conditions for all Equipment Implemented as part of the SIEM. The Contractor shall include all manuals necessary to manage (e.g., configure, operate) the SIEM

xxii. The Contractor shall guarantee the SIEM, or portions thereof, will not be discontinued by the manufacturer for at least 3 (three) years.

xxiii. The Contractor shall adhere to the OAG's rules for accessing the OAG locations for the SIEM Implementation.

xxiv. The Contractor shall adhere to the OAG's direction with respect to shipping/receiving and storage logistics of Equipment intended to be sent to the OAG.

xxv. The Contractor shall ensure any Implementation activities do not compromise the integrity of OAG property. Any costs to repair damages made to the OAG property by the Contractor will be borne solely and entirely by the Contractor.

xxvi. The Contractor shall ensure all resources directly responsible for managing the Implementation of the Proposed Solution are trained, experienced and properly credentialed personnel to install and test the services. The Contractor shall utilize Industry accepted standards. The Contractor shall collaborate with the OAG, including the OAG contractors, and any others to develop a master schedule for the Implementation.

xxvii. The Contractor shall ensure the SIEM is Implemented by manufacturer certified technicians or specialists.

xxviii. The Contractor shall keep the SIEM service escalation process and contact information current and update the OAG when changes occur. The service escalation process allows the OAG to effectively interface with the Contractor for service, support, maintenance or any other activity with respect to keeping the SIEM working to OAG's expectations.

APPENDIX A: DECLARATIONS AND CERTIFICATIONS (MANDATORY)

The following declarations **MUST** be completed as appropriate and **MUST** be signed by an authorized official. This appendix **MUST** be submitted as part of the Proponents' technical proposal. The OAG **WILL** declare any proposal non-compliant if it is not complete or signed.

A1. PROPONENT'S BUSINESS INFORMATION

As required by Section 1 of this RFP, Proponent's **MUST** supply the following information:

Legal Name of Proponent	
Proponent Business Address (including street address, city, country and postal code or their equivalents).	
Proponent Telephone & Fax Numbers	
Point of Contact for Proposal and any resulting contract (name, telephone and fax numbers and email address).	
Proponents Business Number (PBN) and/or GST/HST number.	

A2. PROPOSAL VALIDITY PERIOD

As required in Section 1 of this RFP, the Proponent certifies that their proposal is valid in all respects for a period of not less than 120 days from the closing date of the RFP.

A3. EMPLOYMENT EQUITY

The Federal Contractors Program for Employment Equity (FCP-EE) requires that some organizations bidding for federal government contracts make a formal commitment to implement the employment equity, as a pre-condition to the validation of their bids. All Proponents must check the appropriate box(es) below. Failure to do so **WILL** render the proposal non-responsive.

Program requirements do not apply for the following reason(s):

[ ] bid is less than $1,000,000.00;

[ ] this organization has fewer than 100 permanent part-time and/or full-time employees;

[ ] this organization is a federally regulated employer;

or, program requirements do apply:

[ ] copy of signed Certificate of Commitment is enclosed; or

Certificate number is:

_____

Note 1: The FCP-EE applies to Canadian-based Proponents only.

Note 2: Organizations that are subject to the FCP-EE but that have been declared ineligible to receive government contracts of goods and services over the threshold for solicitation of bids as set out in the Government Contract Regulations (GCRs) (currently $25,000, including all applicable taxes) by Human Resources Development Canada-Labour (HRDC-Labour), either as

a result of a finding of non-compliance by HRDC-Labour, or following their voluntary withdrawal from the FCP-EE for a reason other than a reduction in their workforce, have been advised by HRDC-Labour that as a consequence of this action they are no longer eligible to receive any government contract over this threshold. Consequently, their certificate numbers have been cancelled and their names have been placed on HRDC-Labour s List of Ineligible Contractors. Bids from such organizations will be considered non-responsive.

The Bidder certifies that it has not been declared ineligible by HRDC-Labour to receive government contracts over the GCR threshold for solicitation of bids (currently $25,000, including all applicable taxes) as a result of a finding of non-compliance, or as a result of having voluntarily withdrawn from the FCP-EE for a reason other than a reduction in their workforce.

The Proponent acknowledges that the OAG shall rely on this certification to award the Contract. Should a verification by the OAG disclose a misrepresentation on the part of the Proponent, the OAG shall have the right to treat any contract resulting from this bid as being in default, and to terminate it pursuant to the default provisions of the Contract.

A4. CERTIFICATION OF EDUCATION AND EXPERIENCE

The Proponent certifies that all statements made with regard to the education and the experience of individuals proposed for completing the subject work are accurate and factual, and we are aware that the OAG reserves the right to verify any information provided in this regard and that untrue statements may result in the proposal being declared non-responsive or in other action which the OAG may consider appropriate.

A5. CERTIFICATION OF AVAILABILITY AND STATUS OF PERSONNEL

A5.1 Availability of Personnel:

The Proponent certifies that, should it be awarded a contract as a result of this solicitation, the Proponent's resources who are to be assigned to a given project will be available to commence performance of the work within seven (7) days, and will remain available to perform the work.

A5.2 Status of Personnel:

If the Proponent has proposed any person in fulfillment of this requirement who is not an employee of the Proponent, the Proponent hereby certifies that it has written permission from such person (or the employer of such person) to propose the services of such person in relation to the work to be performed in fulfillment of this requirement and to submit such person's résumé to the OAG. As well, the Proponent hereby certifies that the proposed person is aware that overtime may be required and is willing to comply.

During the bid evaluation, the Proponent **MUST**, upon the request of the OAG, provide a copy of such written permission, in relation to any or all non-employees proposed. The Proponent agrees that failure to comply with such a request may lead to disqualification of the Proponent's proposal from further consideration.

A6. CERTIFICATION OF FORMER PUBLIC SERVANT IN RECEIPT OF A PENSION

Is the Proponent a former public servant (FPS) in receipt of a pension under the Public Service Superannuation Act (PSSA)?

Yes ( ) No ( )

If so, the Proponent must provide the following information:

a. Name of public servant

b. Date of termination of employment or retirement from the Public Service

If the Proponent is a former public servant in receipt of a pension under the PSSA, the Proponent acknowledges and agrees that the contract with the Auditor General will be reported on the OAG website as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

A former public servant under PSSA (*) is defined as:

a. An individual,

b. An individual that has incorporated,

c. A partnership made of former public servants in receipt of PSSA pensions

d. A sole proprietorship or entity where the affected individual has a controlling (**) or major (50% + 1) interest in the entity,

(*) It does not include pensions payable pursuant to Canadian Forces Superannuation, Defence Services Pension Continuation, Royal Mounted Police Superannuation, Members of Parliament Retiring Allowances and Canada Pension Plan

(**)For this purpose, “controlling” includes everyone, but not limited to organizations, bodies corporate, societies, companies, firms, partnerships, associations of persons, where individuals or directors, directly or indirectly either controls or has the power to control the other(s).

Work Force Reduction Program

Is the Proponent a FPS who received a lump sum payment pursuant to the terms of a work force reduction program? **Yes ( ) No ( )**

If so, the Proponent must provide the following information:

a. Name of public servant

b. Conditions of the lump sum payment incentive

c. Date of termination of employment

d. Amount of lump sum payment

e. Rate of pay on which lump sum payment is based

f. Period of lump sum payment including start date, end date and number of weeks

g. Number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program

A lump sum payment period means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including the Goods and Services Tax or Harmonized Sales Tax.

A7. CERTIFICATIONS IN ACCORDANCE TO THE REQUIREMENT FOR THE SET-ASIDE PROGRAM FOR ABORIGINAL BUSINESS

A3000C

1. The Proponent warrants that its certification of compliance is accurate and complete and in accordance with the "Requirements for the Set-aside Program for Aboriginal Business" detailed in Annex 9.4 of the *Supply Manual*.
2. The Proponent must keep proper records and documentation relating to the accuracy of the certification provided to Canada. The Proponent must obtain the written consent of the Contracting Authority before disposing of any such records or documentation before the expiration of six (6) years after final payment under the Contract, or until settlement of all outstanding claims and disputes, under the Contract, whichever is later. All such records and documentation must at all times during the retention period be open to audit by the representatives of Canada, who may make copies and take extracts. The Proponent must provide all reasonably required facilities for any audits.
3. Nothing in this clause must be interpreted as limiting the rights and remedies which the OAG may otherwise have pursuant to the Contract.

A3000T

1. This procurement is set aside under the federal government's Procurement Strategy for Aboriginal Business, as detailed in Annex 9.4, Requirements for the Set-aside Program for Aboriginal Business, of the *Supply Manual*.
2. The Proponent:
    i. certifies that it meets, and will continue to meet throughout the duration of any resulting contract, the requirements described in the above-mentioned annex;
    ii. agrees that any subcontractor it engages under any resulting contract must satisfy the requirements described in the above-mentioned annex; and
    iii. agrees to provide to the OAG, immediately upon request, evidence supporting any subcontractor's compliance with the requirements described in the above-mentioned annex.
3. The Proponent must check the applicable box below:
    - ( ) The Proponent is an Aboriginal business that is a sole proprietorship, band, limited company, co-operative, partnership or not-for-profit organization.
    - **OR**
    - ( ) The Proponent is either a joint venture consisting of two or more Aboriginal businesses or a joint venture between an Aboriginal business and a non-Aboriginal business.
4. The Proponent must check the applicable box below:
    - ( ) The Aboriginal business has fewer than six full-time employees.
    - **OR**
    - ( ) The Aboriginal business has six or more full-time employees. The Proponent must, upon request by the OAG, provide all information and evidence supporting this certification. The Proponent must ensure that this evidence will be available for audit during normal business hours by a representative of the OAG , who may make copies and take extracts from the evidence. The Proponent must provide all reasonably required facilities for any audits.

5. The Proponent must, upon request by the OAG, provide all information and evidence supporting this certification. The Proponent must ensure that this evidence will be available for audit during normal business hours by a representative of Canada, who may make copies and take extracts from the evidence. The Proponent must provide all reasonably required facilities for any audits.

A3001T

If requested by the Contracting Authority, the Proponent must provide the following certification for each owner and employee who is Aboriginal:

1. I am _____ (*insert "an owner" and/or "a full-time employee"*) of _____ (*insert name of business*), and an Aboriginal person, as defined in Annex 9.4 of the *Supply Manual* entitled "Requirements for the Set-aside Program for Aboriginal Business".

2. I certify that the above statement is true and consent to its verification upon request by the OAG.

AUTHORIZED SIGNATORY

By submitting a proposal and signing below, the Proponent certifies that the information submitted in response to the above requirements is accurate and complete. Proposals must be signed to be evaluated.

AUTHORIZED SIGNATORY			
SIGNATURE:		**DATE:**	
NAME OF OFFICIAL (please print)			

APPENDIX B: MANDATORY REQUIREMENTS CHECKLIST—CONTRACTING

Proponent's **MUST** complete the following table and submit it as part of their technical proposal.

Item	MANDATORY REQUIREMENTS	Compliant?		Location in Proposal
		Yes	No	
MC-1	Proposals **MUST** be received as per the instructions in Section 1.			N/A
MC-2	Proponents **MUST** complete and sign all certifications required in Appendix A of this RFP and attach them as Appendix A of their technical proposal.			
MC-3	Proposals **MUST** be organized and comply with the proposal structure and page limit (60 pages), as described in Section 3.			
MC-4	Proponents **MUST** complete and include this table as part of their Technical Proposal.			
MC-5	Proponents **MUST** provide the full cost of their proposed software (including option years) using the chart formats provided in Sections 3.4.			
MC-6	Proponents **MUST** provide one or more references as described in CR-04 (Appendix C)			

APPENDIX C: EVALUATION CRITERIA AND SCORING GRID

Proposals meeting the mandatory requirements will be evaluated using criteria and scoring systems described below.

Req. Identifier	Rated Requirement	Maximum Points	Score
CR-01	**Assessment of Escalation Process.** Proponents are to describe their support model, their escalation process and contact information to be used in the event of problems (during Implementation and post-Implementation of the SIEM) or any other OAG requests. The description of the support model must clearly identify the key elements required to provide user support.	**25**	
CR-02	**Assessment of Quality System.** Proponents should have a rigorous Quality Assurance methodology to ensure the accuracy, ease of use, security and quality of the proposed solution. Proponents are to describe how they ensure the quality of the Equipment provided in their solution including maintenance fixes and updates. A measurement of process maturity that determines effectiveness in delivering quality product (hardware/software) is in use; for example, Information Technology Infrastructure Library (ITIL) or International Organization for Standardization (ISO).	**25**	
CR-03.1	**Assessment of Proponent's Financial Stability, Experience and Support Capabilities**. Proponents are to provide a brief history of the company, including financial stability and experience in the manufacturing, implementation and support of the proposed Solution. In addition: ➢ If the Proponent does not manufacture the proposed solution, the Proponent must provide the manufacturer's name and Proponent/manufacturer relationship. ➢ If the Proponent does not provide installation, warranty or maintenance services, the Proponent must explain the Proponent/manufacturer/subcontractor responsibilities including future support for proposed Solution.	**25**	
CR-03.2	Proponents are to describe their experience gained implementing like SIEM solutions in other projects for similar types of environments. Proponents are to provide details on how the experience gained during these projects will enhance the successful delivery of this Solution. The Proponent should have Enterprise Security or IT / Information Security as one of their primary business line. ➢ 75 points for greater than 8 similar Solutions Implemented; ➢ 50 points for 5-7 similar Solutions Implemented; ➢ 25 points for 3-4 similar Solutions Implemented; ➢ 0 points for <3 similar Solutions Implemented.	**75**	

Req. Identifier	Rated Requirement	Maximum Points	Score
CR-03.3	Proponents are to describe their availability for 24-hour, 7 day a week support and describe remote and on-site capabilities.	**25**	
	Subtotal for CR-03:	**125**	
CR-04	**Assessment of the Reference Sites**. Proponents are to provide detailed information on three reference sites whose requirements are similar to the SIEM solution the OAG is requesting. The response should include the following information: name, telephone number and e-mail address of the project authority and year the solution was implemented (see Section 2.8 for suggested table format). ➢ 100 points if all three (3) references have implemented similar solutions to the OAG ➢ 75 points if two (2) references have implemented similar solutions to the OAG ➢ 50 points if one (1) reference has implemented similar Solution to the OAG ➢ 0 points if no reference has implemented similar Solution to the OAG References may be contacted to help validate claims made by Proponents and to seek feedback on the quality of the solutions and services provided by the Proponent. References may be contacted during any phase of the evaluation process.	**100**	

Product Architecture		Maximum Points	Minimum Score	Score
TR-01 Deployment				
	Proponents are to describe how they will Implement the proposed SIEM Solution to connect to the various network elements and meet the capacity, functionality and feature requirements outlined in Sections 2.2 and 2.4. In addition, the proposed solution must provide the following capability: • Fully centralized (central collection, central analysis & alerting. The proposed solution should also be deployed using either: • Appliance-Based (fully centralized) or • Virtual machine-based (virtual appliances for collection and analysis & alerting) If the proposed solution is appliance-based, Proponents are to	**50**		

	indicate any internal redundancy/resiliency capabilities (i.e. internally redundant hardware) and external redundancy/resiliency capabilities (i.e. failover devices) that are part of, or can be made part of the proposed solution.			
TR-02 Infrastructure/Licenses				
TR-02.1	Based on the provided enterprise description, Proponents are to indicate how many collectors/aggregators/analyzers and what type (if the proposed Solution is based on point capability solutions) will be required for optimal levels of network protection. Proponents should also provide justification for that number of devices/licenses. Where multiple devices/licenses are required, Proponents should indicate which model is necessary in each specific case and provide justification for that model of device/license.	**40**		
TR-02.2	Proponents are to indicate all of the licensing details for the proposed Solution, such as whether it is periodic or perpetual, whether it is licensed by seat, IP address, named-user or by events per second.	**20**		
	Subtotal for Infrastructure/Licenses:	**60**		
TR-03 Supporting Devices				
	Proponents are to indicate whether the proposed Solution requires a separate and/or dedicated reporting device/license. If a separate and dedicated reporting device/license is not required, but one is available, indicate the reporting enhancements provided by this device/license. **Ideally**, the solution does not require a separate and/or dedicated reporting device/license.	**40**		
TR-04 Scalability				
	Proponents are to indicate the degree to which the proposed Solution can be scaled. Indicate both the degree to which an individual collector/aggregator/analyzer can be scaled (that is, have its performance increased/enhanced without being replaced), as well as the degree to which the system as a whole can be scaled (that is, the number of individual collectors/aggregators/analyzers that can be effectively managed via the management interface).	**40**		
TR-05 System Integration				
	The Proponent's proposed solution should indicate which type(s) (if any) of the following enterprise solutions it can	**100**	**60**	

	integrate with without customization (i.e. out of the box): • Perimeter anti-malware solutions • Firewall/UTM solutions • Intrusion detection/prevention solutions • Managed network switches • Managed routers • Application servers (application logs) • Database servers (database logs) • Web servers • Communications servers (email, unified communications, VOIP, etc….) • Workstation security solutions (anti-virus, anti-malware, desktop IDS, etc....) • Identity and Access Management systems • Configuration Management Database • Workstation and server operating systems			
TR-06 Data Connectors				
	The Proponent's proposed solution should describe and demonstrate how the Proponent will implement data connectors for devices, software and other technologies existing within the OAG network, which are not immediately compatible with the proposed solution.	**40**	**20**	

Product Features		**Maximum Points**	**Minimum Score**	**Score**
TR-07 Collection/Aggregation/Normalization				
	The Proponent is to indicate whether the proposed solution supports the following capabilities. Describe the specific capability in that area: • Sflow data and data sources • Identity data and data sources • Client/server application-specific data and data sources • Web-based application-specific data and data sources • Database-specific data and data sources • Configuration data and data sources • File integrity data and data sources	**50**		

	The solution should store event/log data in a compressed manner and should have features that support different retention requirements for various data/event logs under the scope. The solution should be capable of collecting event data over a secure channel. At a minimum, the proposed Solution should : • Support automated discovery of information processing equipment/devices, through an agent-less deployment. • Capable of discovering new information processing equipment/devices, added to the existing scope. • Support automated timestamp synchronization through standard Network Time Protocol (NTP). • Capable of detecting inconsistencies/variations in the source time stamp and provide meaningful / right information for correlation. • Recognize and record, including but not limited to, the following properties associated with an asset: o name of the asset o owner of the asset o location of the asset (based on port numbers and switches) o software/applications/configurations associated with the asset o type of the asset (server, desktop, laptop, router, switch, IP Telephone, etc.)			
TR-08 Correlation				
	The Proponent is to indicate whether the proposed solution supports the following correlation capabilities. Proponents should describe the specific capability in that area: • Correlation according to canned policies • Correlation according to user-defined policies o Via GUI o Via natural language o Via script or formula-like functions • Correlation according to adaptive/heuristic policies • Correlation rule creation via GUI Based on the criticality of event and asset under consideration, the solution shall be capable of classifying /identifying anomalies and performance issues. Results of correlations shall provide meaningful information of anomalies, with respect to the affected / involved system(s). The Solution should be capable of integrating with other security infrastructures of the OAG (like vulnerability management solution, firewall, intrusion preventions system, end-point security solutions, etc.) to correlate and provide a central dash-board to manage all security related anomalies. Based on the criticality of event and asset under consideration, the Solution should be capable of classifying /identifying	**40**		

	anomalies and performance issues. Results of correlations should provide meaningful information of anomalies, with respect to the affected / involved system(s). The Solution shall consider the following : • Distinguish between authorized privileged operations and anomalies, to provide correct / appropriate / meaningful information. • User actions should be able to be considered by the solution, while performing correlation of event data. • Failed authentication request. • Failed resource access (authorization) • Failed access attempts, with respect to, application-to-application / application-to-system / application-to-backend / web-to-application and/or vice versa. • Successful logons, after consecutive failed access attempts. • Network failures and floods • Consider start-up / start & shut-down / stop of system(s) and service(s). • Changes in the operating environment should be considered during correlation. The following type of changes, at a minimum, are to be considered: o System state o Operating systems o Application o Database o Configuration files o Network & security infrastructures o Privileges o Access methods			
TR-09 Analysis				
	Proponents are to indicate whether their proposed solution supports the following analytics capabilities. Describe the specific capability in that area: • Natural language custom querying • Custom querying via script or formula-like functions • Data drill-down via GUI Solutions should provide for deep data analysis, so as to generate meaningful information to satisfy requirements of: • Management reporting • Addressing security and operational anomalies • Protocol analysis • Compliance and audit reporting • Forensic analysis • Trend analysis & predictions • Bench marking	**40**		

	• Anomaly identification with respect to most affected system, mostly present incident type, etc. • Detailed reporting			
TR-10 Data Management				
TR-10.1	Proponents are to indicate whether their proposed solution supports the following management capabilities. Describe the specific capability in that area: • Role-based access control to the solution as a whole • Role-based access control to specific capabilities, functions and/or repositories within the solution • Encryption of all data within remote collectors/aggregators and analyzers, where such devices are port of the proposed solution • Encryption of all data within local collectors/aggregators and analyzers • Encryption of all communications between collection points and storage repositories At a minimum, proposed solutions should have their own role-based user management module with capabilities to assign and manage privileges, and should support integration with Microsoft standard identity & access management.	**20**		
TR-10.2	Proponents are to describe the data retention capabilities inherent within their solution. Descriptions should address the following: • Indicate whether your solution allows for hierarchical storage management such that active data can be retained for real-time investigation and historical data can be retained for as required investigation. • Where the capability exists, indicate the volume of active data that can be stored within the system (expressed in correlated events) for real-time access. • Where the capability exists, indicate the volume of historical data that can be stored within the system (expressed in correlated events) for as required access.	**20**		
	Subtotal for Data Management:	**40**		

Product Operations	**Maximum Points**	**Minimum Score**	**Score**
TR-11 Implementation and Configuration			

	Proponents are to describe and demonstrate how they will Implement a fully functional SIEM with the following specifications: • Capacity for 200 server class devices of varying Windows, Unix and Linux operating systems • Capacity for 100 layer 2 network devices • Capacity for at least 150 events/second sustained • Capacity for a minimum peak rate of 23000 events/second • Near-real-time management • Real-time events analysis • Correlation of data from disparate sources/sensors • Real-time correlation with a minimum of 90% accuracy at established events per second • Normalization of data from disparate sources/connectors • Log/data retention for a minimum of 90 days • Ability to utilize either a native database, networked database or SAN technology • Compression of log data with a target compression ratio of 8:1 • SIEM data is encrypted using AES with minimal impact on access • Correlation rules and alerts are user-configurable • Correlation rules and alerts are configurable via a GUI • Data connectors available for common operating system and network elements	**100**	**70**	
TR-12 On-Going Operations				
	Proponents are to describe: • The process by which the initial configuration of the proposed solution is performed. Include the implementation of any signature database(s), the creation of any rules, and the configuration of any and all settings required for optimal operations. • The process by which the initial configuration is update and maintained. Include the update of any signature database(s), the update and/or modification of any rules, etc.... The OAG is looking for a solution that is easy to maintain and does not require the analyst to log in continuously. Reports may be reviewed weekly or monthly and should not require extensive customization. The proposed SIEM Solution is expected to be as close as possible to an automated Security Operations Center (SOC). The Solution must be easily configurable based on rules. The analyst should never have to log in unless there is a need to investigate alerts, review reports or perform other similar tasks. Proponents are to demonstrate that their proposed solution provides a simple interface for managing day-to-day tasks “out of	**75**	**45**	

	the box." A simple interface can be described as an interface that requires a minimal number of mouse clicks for a user to perform specific tasks. For example, a user should not have to navigate through multiple screens to access information, to adjust configuration items or to define security/policy/rule. A simple user interface should be: • Explorable: provides safe cancel and roll-back features with simple, visible and straightforward navigation. • Intuitive: the users can easily guess at the meaning and behavior of the features or capabilities. • Guiding: the appearance and organization of the interface easily guides the users through tasks, which can include intrinsic help and/or informative feedback integrated within the interface. • Predictable: consistent behavior and appearance throughout.			
TR-13 Alarming and Alerting				
	Proponents should describe the process by which the management console can be configured to issue alarms and alerts: • Detail the different alarming/alerting mechanisms that can be configured and the manner in which they can be configured. • Indicate whether the solution can integrate with third-party ticketing and workflow systems. Where integration is possible, indicate which platforms the proposed solution integrates with and describe the integration process. At a minimum, the alerting mechanism shall be able to: • Send repeated alerts, until such time as the incident is addressed or has been turned-off by authorized resources. • Provide means for escalations, when the alerts are not addressed within stipulated time window, for various identified category of alerts. • Provide manual alerting mechanism, used by administrators to manually raise alerts during discovery of anomalies, using custom alerts. • On a real-time basis, alert the administrator(s) or nominated person, on identification/discovery of new information processing equipments or devices. • Provide the capability to generate trend analysis reports.	**40**		
TR-14 Auditing and Reporting				
	Proponents should describe the auditing and reporting capabilities for captured logs and events. They should: • Address whether standard report templates exist, whether	**40**		

	they must be constructed, or whether the system supports ad hoc reporting only. Where standard templates exist, indicate what types of reports they represent and in all cases indicate what types of information can be presented in reports. Specify if specific compliances mandates can be reported against; • Indicate whether their proposed solution can integrate with third-party reporting solutions. Where integration is possible, indicate which platforms the proposed solution integrates with and describe the integration process; • Indicate whether their proposed solution can produce a pictorial representation of the anomaly detected, highlighting all involved components and affected systems /applications/ services; and, • Indicate whether their proposed solution provides for the export of log/event data (selective or complete). The reporting capabilities should be able to provide the following at a minimum: • Capabilities to provide executive reports, of events/incidents, in a pictorial representation; • Reports based on individual system; • Reports based on specific service; • Reports based on specific events/incidents; • Reports based on application(s) in use; • Reports based on location; • Reports based on source & target; • Reports based on specific timing/duration; • Reports based on priority / criticality of the events/incidents; • Reports based on impact (system / service / application/infrastructure unavailability); • Reports based on ownership of system / equipment/application/service; • Reports based on changes to system / equipment/application/service; • Reports on exploited systems/equipment/application/service; and • Reporting formats – at least two of the following formats "PDF, MS Excel, HTML & plain text"			
TR-15 Backup and Recovery				
TR-15.1	Proponents are to describe, for each major component of the SIEM, the mechanism (and storage medium) for backing-up the software and configuration files; the time (duration) of the back-up should also be included. Proponents are to describe how the SIEM is restored from back-up files. Proponents should also include Implementation services to assist the OAG in setting up these back-ups; using existing OAG data storage equipment.	**10**		

TR-15.2	Proponents are to describe the process (including durations) to recover the SIEM from a complete power outage situation.	**10**		
TR15.3	Proponents are to describe the processes by which the command console can be backed up. Descriptions should address whether the back-up process in any way compromises operations and/or security.	**10**		
TR-15.4	Both backup and recovery should allow for full and incremental notions of backup to reduce the time and backup media requirements needed to perform storage of system state information. Incremental and full backup images of system state information can be stored on the proposed solution, but should be able to be downloaded from the system for storage external to the solution and to support off-site storage of backup images.	**10**		
	Subtotal for Backup and Recovery:	**40**		

Project Management and Implementation		**Maximum Points**	**Score**
TR-16 Project Management			
	Proponents are to provide a dedicated project manager/lead for the duration of the Implementation of the SIEM proposed Solution. Proponents should provide credentials and a CV of the project manager/lead along with references related to projects of similar complexity that the project manager has been involved with.	**10**	
TR-17 High Level Project Plan			
	Proponents should provide, in their response, a project plan, showing the high level activities, key dates, time frames, resources and dependencies for procuring and Implementing the SIEM proposed Solution. The project plan will be used as a basis to establish the mutually agreed upon project implementation schedule and to establish a matrix for discounts for Contractor project delays.	**10**	
TR-18 Testing Process			
TR-18.1	Proponents should have a standard test methodology and documented process for testing proposed SIEM Solutions. Proponents are to provide a high-level test plan including the types of tests and measurements that will be performed to validate the proposed Solution. Included in the test plan should be the expected outcome of the tests to be performed.	**15**	

TR-18.2	Proponents should provide the OAG with a written Test Notification. The Test Notification should describe the proposed test(s) to be demonstrated and the SIEM solution component(s) to be tested.	**15**	
	Subtotal for Testing Process:	**30**	
TR-19 Commissioning Process			
TR-19.1	Proponents should have a standard methodology and documented process for commissioning the proposed Solution. Proponents should provide a high-level plan including the types of activities that will be performed to commission the proposed SIEM Solution.	**10**	
TR-19.2	The plan should have defined steps with specific milestones covering all critical elements of the commissioning process. Included in the commissioning plan should be the expected outcome of the activities to be performed.	**10**	
	Subtotal for Commissioning Process:	**20**	

Training and Transition		**Maximum Points**	**Score**
TR-20 Training Program and Documentation			
TR-20.1	Proponents are to describe their training program and documentation process. As a minimum, Proponents are to include descriptions of the following subjects in their proposal: • How the quality of hardware/software documentation is assured; • How technical training is provided to both end-users and personnel (network, workstation and security administrators) who will be administrating the solution. The Successful Proponent will conduct end-user training, tailored specifically to the audience (e.g. network, workstation and security administrators). Please describe end-user training available and identify what is included in the proposed solution.	**20**	
TR-20.2	For administrators, Proponents are to support both online training and off-site classroom training. Proponents should describe online and off-site training capabilities. Proponents should also indicate any recommended administrator classes.	**5**	
TR-20.3	Proponents should provide the OAG a copy of the system drawings necessary for the proper utilization of the proposed solution. These shall include but are not limited to:	**5**	

	• System drawing including appropriate IP addressed for critical components and troubleshooting. • Operating procedures and methods including diagnostic and test procedures.		
TR-20.4	Proponents are to describe how they will ensure that the quality of the documentation material or user interface provided to the OAG as part of their proposed solution is of the highest quality. This description should include a description of how they ensure the quality of the French translation of this material, if available. Proponents should also describe their approach to ensuring that high quality materials will be available to the OAG in both official languages for maintenance fixes and updates.	**15**	
	Subtotal for Training and Documentation:	**45**	
TR-21 Transition Support Program			
	Proponents are to describe how they would assist the OAG with technical staff readiness.	**20**	

Post Implementation Support and Maintenance		**Maximum Points**	**Score**
TR-22 Warranty			
	Proponents are to describe the warranty program included as part of their proposed solution. The OAG expects that all maintenance during the warranty period and under any maintenance agreements will be performed by the Successful Proponent using qualified personnel at no additional cost to the OAG other than those charges identified in the applicable warranty/maintenance agreement.	**10**	
TR-23 Maintenance and Support			
TR-23.1	Proponents should provide their standard service level agreement including hardware replacement time frames (e.g., mean-time-to-acknowledge, mean-time-to-respond and mean-time-to-repair). Proponents should also provide samples of all software licence agreements that would apply as part of their proposed solution.	**10**	
TR-23.2	The OAG expects that the Successful Proponent will provide a 24-hour a day, 7-day a week support center, as well as online service capabilities. Proponents should include descriptions of the support	**10**	

	services they provide, At a minimum their proposal should address the following subjects: • Toll-free telephone support; • Any online (web) service request capabilities available to the OAG; • On-site support when required; • Technical support for upgrading the solution; • Versions\updates are released at regular intervals; and, • French and English language support.		
	Subtotal for Maintenance and Support:	**20**	
TR-24 Hardware Replacement and Sparing			
TR-24.1	Proponents should describe the impact to end-user service availability when replacing faulty major hardware components.	**5**	
TR-24.2	Proponents should provide a hardware sparing strategy, for the proposed SIEM solution that balances on-site purchased spares versus a managed spare replacement (and Implementation) service.	**5**	
	Subtotal for Hardware Replacement and Sparing:	**10**	
TR-25 Scheduled Maintenance			
TR-25.1	Proponents should list, for each major system component of the proposed SIEM Solution, the expected scheduled maintenance activity and the impact to service or service feature availability of this activity.	**5**	
TR-25.2	Proponents should include the estimated time and/or manual effort involved in the scheduled maintenance activity in question (e.g., software upgrades, software fix/feature applications, hardware replacement/upgrades, and configuration changes).	**5**	
	Subtotal for Scheduled Maintenance:	**10**	

APPENDIX D: PILOT SCENARIOS

DESCRIPTION OF SCENARIO	REMARKS
Scenario 1 - Log source configurations **Goal:** To demonstrate the process of adding and configuring various log data source systems. This will verify requirements described in TR-05, TR-06. Basic log data sources a) Demonstrate the process by which a standard log source (e.g. device *syslog*) is added to the SIEM system. b) Demonstrate the configuration of global and source-specific log retention settings and "log source unavailable" alerting. Enriched log data sources, the log info must be able to obtain context information, such as: a) What is the system IP address (other names, location in the network, etc) b) Identification of the service Confirmation of data from source (e.g. Microsoft AD, firewalls, workstations, network switches, etc.). a) Demonstrate that sources, as described in TR-05, can be added to the SIEM system without customization. b) Demonstrate event data enrichment using newly-added log data sources. c) Demonstrate how the information from the data source is used. d) Demonstrate where the data is in relation to the network flow. e) Demonstrate the process to normalize custom log records.	
Scenario 2 - Event correlation, alerting, log analysis, and incident management **Goal:** To demonstrate Solution capabilities for event correlation, alerting, associated log data analysis, and event/incident workflow management. This will verify requirements described in TR-07, TR-08, TR-09. Standard events a) Demonstrate the process by which a standard event correlation policy is configured in the system, including assignment of custom severity levels. b) Demonstrate the options for initial and escalated alerting of the event within the SIEM product, and	

through e-mail notification. c) Demonstrate the ability to perform additional log data analysis based on details of the correlated event. d) Demonstrate the ability to track event management/incident response activity for the event. Threshold-based events a) Demonstrate the ability to set and adjust threshold-based correlation policies. Custom event correlation a) Demonstrate the ability to create custom correlation policies.	

Scenario 3 - Reporting features **Goal:** To demonstrate Solution capabilities for reporting and report review tracking. This will verify requirements described in TR-09, TR-13, TR-14. Standard reporting features a) Demonstrate the process by which a standard report is generated, and options for distribution of the report to end users. b) Demonstrate the process by which activity associated with a specific event or incident is formatted into a report. c) Demonstrate the process of generating a custom report. Advanced reporting features a) Demonstrate the ability to report on mandatory log review activity. b) Demonstrate the ability to integrate with external reporting platform [e.g. Crystal Reports, Cognos BI, etc].	
Scenario 4 - Dashboard and access control features **Goal:** To demonstrate Solution capabilities for customized access and display. This will verify requirements described in TR-11 and TR-12. The SIEM solution takes less than 2 days to install and configure for use. Demonstrate that the Solution allows users to fully customize graphical dashboards. Demonstrate that the GUI requires minimal amount of mouse clicks to perform routine tasks, such as generating reports, viewing critical information at a glance. The user interface must be capable to provide unified data presentation (UDP), including content information. See TR-12. Granular access control features a) Demonstrate the ability to restrict access to specific product modules (e.g. reporting) and components (e.g. specific reports). b) Demonstrate the ability to restrict access to specific log data sources (e.g. PCI-grouped devices). Customized display a) Demonstrate the ability to customize user dashboard elements. b) Demonstrate dynamic and context-based updating of dashboard elements.	