Office of the Superintendent of
Financial Institutions Canada

Bureau du surintendant des
institutions financières Canada

Request for Information

FOR

**The Office of the Superintendent of Financial Institutions'
Managed Security Services Provider**

Date Issued:**August 15, 2017**

Response Period Closes: **September 26, 2017**
File Reference Number: **OSFI MSSP-2017**

Address Inquiries to:

Isabelle Legault
Senior Contracting Officer
Office of the Superintendent of Financial Institutions
Telephone: 613-949-6807
E-mail: contracting@osfi-bsif.gc.ca

Return Responses to:

Isabelle Legault
Senior Contracting Officer
Office of the Superintendent of Financial Institutions
Telephone: 613-949-6807
E-mail: contracting@osfi-bsif.gc.ca

OSFI
BSIF

Canada

REQUEST FOR INFORMATION

TABLE OF CONTENTS

SECTION I

INTRODUCTION AND PROCESS FOR RESPONDING TO THE REQUEST FOR INFORMATION

Requirement

The Office of the Superintendent of Financial Institutions (OSFI) is planning to seek funding for a Managed Security Services Provider (MSSP) to provide various security operational and monitoring services on a 24 x 7 x 365 basis. Once the business case and associated funding are approved, OSFI plans to conduct a Request for Proposal (RFP) to procure services relating to security operations and monitoring.

The main objective of this initiative is to notify Industry of OSFI’s intentions with respect to the MSSP Project and solicit feedback regarding their experience with this type of initiative and obtain:

a) regarding description of each of the services offered by managed security service providers including, and how those services would typically be integrated into OSFI’s existing security architecture and operational capability; and,

b) a rough order of magnitude estimate on costs for implementation and ongoing operations, which will help OSFI to secure necessary funding.

Background

The Office of the Superintendent of Financial Institutions (OSFI) is the primary regulator of federally chartered financial institutions and federally administered pension plans. OSFI's mission is to protect the rights and interests of depositors, policyholders, pension plan members and creditors of financial institutions, and to advance and administer a regulatory framework that contributes to public confidence in a competitive financial system. OSFI supervises and regulates all banks, and all federally incorporated or registered trust and loan companies, insurance companies, cooperative credit associations, fraternal benefit societies and pension plans.

As Cyber Security becomes an ever-increasing priority for OSFI, it has become important to not only prevent cyber-attacks, but also to detect, contain, and eradicate cyber threats to OSFI networks through monitoring, intrusion detection/prevention, and application of protective security services to OSFI information systems.

OSFI's Cyber Security is responsible for the provision of security services such as policy development, security training and awareness, risk management, security assurance, and incident management for the Agency. Currently the Security Operations Centre (SOC), including security monitoring and operations reports to the Director, Infrastructure and Technology Services. As part of the scope of the business case development, a review of all functional responsibility and associated funding for these activities is planned to take place.

OSFI anticipates a requirement for a single contractor to provide professional services to setup, manage, operate and maintain the SOC services and associated technology to enable OSFI to prevent, detect, and respond to cyber security threats. The core services to be acquired under this proposed RFP could include 24 hours per day, 7 days per week, 365 days per year (24x7x365) threat intelligence and reporting, network monitoring and security event triage, analysis, and alerting, and computer security incident response/support. Additional services such as on-site incident management support, ongoing vulnerability assessments, security technology management and support (such as firewall, perimeter and endpoint security technology, etc) and forensics services in support of an investigation could also fall within the scope of the planned RFP.

Detailed information about the Office of the Superintendent of Financial Institutions (OSFI), including our mission and objectives, history, organization and how we regulate can be found at OSFI's website www.osfi-bsif.gc.ca.

Nature of the Request for Information

This is not a bid solicitation. This Request for Information (RFI) will not result in the award of any contract. Potential suppliers of any goods or services described in this document should not earmark stock or facilities, not allocate resources, as a result of any information contained herein. This Industry Research Initiative will not result in the creation of any source list; therefore, whether or not any potential supplier responds to this request will not preclude that supplier from participating in any procurement related to this initiative. Also, the procurement of goods or services described in this document will not necessarily follow this RFI. This RFI is simply intended to solicit feedback from Industry with respect to the matters described in this document.

Submission of Responses

1. **Time and Place for Submission of Responses.** Interested respondents should submit responses electronically (via email) to the OSFI Contracting Authority identified below. Responses must be received by the time and date indicated on page 1 of this document.

2. **Responsibility for Timely Delivery.** Each respondent is solely responsible for ensuring the response is delivered on time to the correct location. Responses may be submitted electronically as indicated.

3. **Identification of Response.** Each respondent should ensure that its name and return address, the reference number and the closing date are clearly identified in the response.

4. **Return of Response**. Responses to this RFI will not be returned.

5. **Content of Responses.**
   a. Respondents should respond to the questions contained in Section III using the same numbering format.
   b. Respondents are reminded that this is an RFI and not an RFP and, in that regard, respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this document could be satisfied. Any marketing or promotional information submitted as part of the responses will not be reviewed.
   c. Responses will not be used for competitive or comparative evaluation purposes however, for ease of use and in order that the greatest value be gained from responses, OSFI requests that respondents follow the structure outlined below.

Response Costs

OSFI will not reimburse any respondents for expenses incurred in responding to this RFI.

Treatment of Responses

1. **Use of Responses.** Responses will not be formally evaluated. However, the responses received may be used to assist OSFI in the development or modification of the MSSP business case and development of the procurement strategies and RFP requirements. OSFI will review all responses received by the deadline. OSFI may in its discretion, review responses received after the deadline.

2. **Review Team.** A review team composed of representatives from OSFI will review the responses. OSFI reserves the right to hire any independent consultant, or use any Government resources that it deems necessary to review any response. Not all members of the review team will necessarily review all responses.

3. **Confidentiality.** Respondents should mark any portions of their response that they consider proprietary or confidential. OSFI will treat those portions of the response as confidential to the extent permitted by the Access to Information Act (ATIP).

4. **Follow-up Activity**. OSFI may, at its discretion, contact any representative to follow-up with additional questions or for clarification of any aspect of a response. OSFI may at its discretion, request a closed meeting with respondents to further discuss their Industry Research Initiative response and recommendations.

Enquiries

Because this is not a bid solicitation, OSFI will not necessarily respond to enquiries in writing by circulating answers to all potential respondents. During the Industry Research Initiative process, OSFI will address only questions pertaining to the research process. Requests for additional information regarding the potential MSSP project (beyond that contained in this document) cannot be accommodated. Respondents with questions regarding this Industry Research Initiative may direct their enquiries to the OSFI Contracting Authority as follows:

Isabelle Legault
Senior Contracting Officer
255 Albert Street, 12th Floor Ottawa, ON K1A 0H2
Telephone | Téléphone: 613-949-6807
Facsimile | Télécopieur: 613-990-0081
E-mail | Courriel: contracting@osfi-bsif.gc.ca

Managed Security Services Provider (MSSP) Preliminary Procurement Timeline

OSFI is contemplating publishing an RFP to procure a Managed Security Services Provider in Q4 of 2017/18. Please note that this is an estimate which has been provided for information purposes only. OSFI reserves the sole option to alter its contemplated procurement schedule as it sees fit.

SECTION II

SCOPE OF POTENTIAL PROCUREMENT AND GENERAL PROJECT INFORMATION

Managed Security Services Provider (MSSP) Project Background

The Strategic Vision for the MSSP project is to "Acquire a security operations and monitoring capability to entirely replace OSFI's existing security operations centre and enhance it". This would include conducting a gap analysis to determine what capabilities and technology would be required, developing and implementing the necessary capabilities and the provision of ongoing security operational and monitoring services.

Scope of Work

Through the potential RFP process, OSFI would be seeking to select a single Contractor to provide support services to setup, manage, operate and maintain a mature Security Operations Centre (SOC) to enable OSFI to prevent, detect, respond and recover from cyber security threats and events. The core services to be acquired under this proposed RFP could include 24 hours per day, 7 days per week, 365 days per year (24x7x365) threat intelligence and reporting, network monitoring and security event triage, analysis, and alerting, and computer security incident response/support. Additional services such as on-site incident management support, security technology management and support (such as firewall, perimeter and endpoint security technology, etc), ongoing vulnerability assessments, and forensics services in support of an investigation could also be in scope of this RFP. Services could also include penetration testing, compliance testing and assessments, digital media forensics, and malware analysis.

Security operations and monitoring

1. Perform continuous monitoring, analysis and reporting of security alerts and event information on a 24x7x365 basis, from all approved security feeds
2. Investigate and positively identify anomalous events detected by security devices or reported to OSFI Cyber Security from external entities, system administrators, and the user constituency
3. Provide notification, escalation, and daily summary reports based on gathered threat intelligence and security event analysis
4. Continuously operate, manage, update and configure all security technology including the Security Information and Event Management (SIEM) System, IDS/IPS, and other potential security technology forming part of the SOC and security operations
5. Monitor and analyze security event data to include investigation of reported incidents using system logs, event correlation between Intrusion Detection Systems (IDS), Data Loss Prevention (DLP), firewalls and other means of detection
6. Review audit logs and record any inappropriate and/or illegal activity in order to reconstruct events during a security incident. This includes monitoring network and host devices and reporting incidents to OSFI Cyber Security staff
7. Provide event analysis and evaluation of the reported incident and provide categorization, prioritization, and recommendation of containment measures
8. Document all event investigation activities, incoming requests for information, or suspected incident reports as required to support the OSFI incident management process
9. Provide written reports detailing all security events and submit these reports, according to established procedures and reporting requirements.

Incident Management Support, Forensics and malware analysis

1. Conduct on-site coordinated computer security incident management, response, and recovery support, as required
2. Perform advanced technical analyses of potentially malicious activities that have occurred or are believed to have occurred on OSFI's network via security event data from the SOC
3. Provide remedial recommendations and produce comprehensive report on findings
4. Perform endpoint/host-based forensics and memory analysis
5. Perform triage and in-depth malware and reverse malware analysis of malicious Windows software and phishing emails, and other client-side exploits, to support the resolution of security incidents
6. Perform digital forensics on media associated with compromised hosts to assess the scope and nature of intrusions
7. Perform remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis and direct system remediation tasks to onsite responders
8. Leverage commercially available and open source forensic tools (e.g. Encase) to efficiently perform forensic analysis
9. Reverse engineer the sequence of events of a breach or attack
10. Perform static and dynamic file analysis to identify malware characteristics, intent and origin
11. Recommend countermeasures to malware and other malicious code and applications that exploit OSFI hosts, endpoints, network and data communication systems
12. Develop recommended changes to policies and procedures that will strengthen the investigative capabilities of malware incidents for the OSFI network infrastructure
13. Advanced code analysis of malicious code detected on OSFI's network, to include offline analysis in an isolated lab environment at the contractor's site
14. Advanced traffic analysis (at the packet level) and reconstruction of network traffic to discover anomalies, trends, and patterns affecting OSFI's networks
15. Provide advanced intrusion detection capability; build, test, and deploy customized IDS and SIEM correlation signatures; monitor daily specialized packet capturing devices onto which those signatures are deployed

Ongoing Vulnerability Assessments and Security Assurance Scans

1. Perform regularly scheduled (monthly and ad hoc) Vulnerability Assessments (VA's) using a master schedule agreed to by OSFI Cyber Security
2. Coordinate the VA testing in advance with Cyber Security to ensure minimal disruption with planned network maintenance, availability, and operations
3. Use approved test procedures, scripts, and VA tools including the latest versions of tools with up-to-date lists of vulnerability checks, appropriate to OSFI's policies, needs and technologies
4. Conduct specialized VA testing to include Database and Web application assessments, penetration testing, and Wireless technology testing and analysis as part of planned security assurance activities or change requests for new or changed systems and architecture
5. Prepare and submit security testing Rules of Engagement (ROE) for approval prior to conducting of penetration testing
6. Employ ad-hoc or emergency VA scanning to support targeted incident investigation, escalation and emergency response to security events in accordance with documented procedures
7. Develop reports, findings, and recommendations to mitigate security gaps and vulnerabilities and provide support to Cyber Security by interpreting scan results and recommend remediation plans
8. Provide VA summary reports of the testing and document the findings

Threat analysis and intelligence

1. Detect, monitor, analyze, and mitigate targeted, highly organized, or sophisticated threats
2. Maintain situational awareness of current activity and risks to OSFI and the GC
3. Leverage all sources of intelligence to develop information on cyber threats and to perform advanced technical analysis on incidents that occur on OSFI networks
4. Perform consolidated and comprehensive information and intelligence analysis of threat data obtained from various sources to provide indication and warnings of impending attacks against OSFI's networks
5. Provide reporting on technical network and host based attack vectors, emerging cyber threats, new vulnerabilities, and current trends used by malicious actors
6. Create and maintain databases to catalog and track ongoing threats to OSFI's networks

Maintain and operate security technology

1. Ensure all SOC systems and applications are available and operational
2. Ensure logging of appropriate security feeds and correlation to the SOC SIEM tool
3. Maintain the Security Information and Event Manager (SIEM) to collect and aggregate Intrusion Detection Systems (IDS) data from network sensors, raw data from collection agents, firewalls, web proxy and content filtering, DLP, antivirus, and vulnerability scanner elements
4. Conduct administration, management, and configuration of the SOC tools (e.g., SIEM, IDS, and DLP, devices and application systems, dedicated servers and sensors)
5. Develop security device signatures, performance reports, and metrics
6. Tune the SIEM and IDS/Intrusion Prevention System (IPS) events to minimize false positives
7. Install or modify network security components, tools, and other systems as required to maintain optimal coverage and performance

Documentation and Standard Operating Procedures

1. Create diagrams of new or revised security deployments before they are transitioned to operational support. This documentation must encompass all systems and applications which comprise and support the SOC.
2. Develop SOC standard operating procedures (SOP) and revise them when changes to SOC operations occur.
3. Provide daily, weekly, and monthly written reports consisting of a summary of all SOC activities, performance metrics, security incident status and actions accomplished for the period.
4. Submit the following reports to Cyber Security;
   a) Program Management monthly status reports on the progress made during the current period
   b) planned activities and problem/issues with recommended solutions,
   c) anticipated delays, and resources expended

Contract Period

OSFI anticipates a multi-year contract, including an initial and option period(s), will be awarded.

SECTION III

QUESTIONS TO INDUSTRY

Respondents are requested to address, but are not limited to, the following questions:

SOC Implementation Strategy and Approach

1) Based on the information that has been provided, and your past experience with similar projects;
    - i. What do you see as the key challenges with this proposed project?
    - ii. What advice can you offer regarding how to structure an RFP and/or contract vehicle to mitigate the risk associated with these challenges?
2) What policies and standards does your organization comply with and how is compliance measured?
3) What are the biggest challenges an MSSP can face when implementing SOC services for a client and what would you recommend clients do to minimize the potential impact, before outsourcing their SOC?
4) It is expected that professional services be included as part of the RFP to assess OSFI's environment and develop a workplan to scope out the work, before services and systems are implemented. Describe your approach for this.
5) Briefly describe the various services that an MSSP can offer to a potential client and what each service might entail.
6) Procurement of Technology:
    - i. Who typically procures, implements, configures, and supports the required technology in an MSSP arrangement?
    - ii. What are the most common technologies being used within the MSSP when providing security monitoring and incident management services?
    - iii. What technology is procured, managed, operated, and supported by the client?(if any); and,
    - iv. Why is it beneficial for the client to manage this technology as opposed to the MSSP?
7) What services/technologies/functions should OSFI have in place and fully mature, before outsourcing a SOC capability? (if any)
8) Can you provide rationale, justification, or financial breakdowns showing why outsourcing a SOC makes financial sense to an organization as opposed to building an internal capability?

Service Level Agreements (SLA's)

9) What service level categories should be considered to ensure efficient detection, analysis and reporting?
10) Have there been any SLA obligations that your organization has found difficult to meet in the past? Why?
11) Can you provide a sample of a typical SLA you have in place with your clients?
12) How do you deal with incidents which are not reported within defined SLA timeframes?

SOC Metrics, Performance, and Reporting

13) What metrics are used to measure SOC performance and/or provide to your clients and how do you present them to your clients?
14) How would you recommend integrating metrics into contractual arrangements?
15) Please provide a sample of typical performance metrics and a sample client report.

Skills and Staffing

16) What certifications and education do you require for your SOC analysts and incident management staff? What minimum certifications should the client expect for all SOC analysts?
17) Do you hire different levels of analysts and if so, what are the minimum requirements (years of experience, education, types of skills) for each level?
18) Does your organization typically subcontract staff or do you maintain internal resources to meet the needs of your clients? If you subcontract, what contingencies do you put in place to ensure sufficient resources are available at all times during the contract?
19) If you maintain internal resources, how do you retain staff? Competitive salaries, bonuses, other forms of compensation?
20) Do you provide specialized training to your SOC staff? If so, please describe level of training, estimated costs per year, numbers of days allocated per staff member per year, etc
21) OSFI requires all staff and Contractors working in the SOC have Government of Canada Secret Clearances. Will this be a problem when trying to outsource to an MSSP?
22) What ratio of number of SOC staff per monitored device is considered typical within an MSSP?
23) Do MSSP’s typically have staff with particular skillsets and experience assigned to particular roles?
24) What skills are considered in highest demand for your SOC analysts and what is your strategy to ensure your staff acquire/maintain these skills?

Project Budget and Schedule

25) Based on the information that has been provided, what do you see as a rough orrder of magnitude (i.e. -25% / +75%) cost estimate be for the MSSP up-front (one-time) costs? What would the rough order of magnitude cost estimate be for ongoing/annual costs?
26) Based on the information that has been provided, what do you see as the approximate overall duration to transition to a fully operational MSSP?
27) OSFI would prefer to leverage fixed-pricing for the contract. Is a fixed-price contract feasible for MSSP arrangements?
28) When new technologies are introduced, how does that get factored into the ongoing costs of the contract?
29) How are changes to the services factored into the ongoing pricing? For example, can devices or data sources be added to the contract without affecting pricing or services?

Incident Management Services

30) Are retainer services for incident management, such as on-site incident response, malware analysis, mitigation, forensics, etc a typical service offering for an MSSP? If so, please describe how the service works including describing the various tiers/level of services offered.
31) Can you provide a rough estimate of pricing for each tier?
32) When using retainer services, how are clients prioritized during an incident? Is it based on the tier/service level or is the client assigned a dedicated team to provide these services within a set timeframe as defined within the contract/SLA?

Data Storage

33) What client data will be collected/captured on the MSSP systems and where is the information stored? How is the information backed up and where is it typically stored? Do MSSP’s typically use hot sites, warm sites, or cold sites for their DR capability?
34) How much data is typically retained by the MSSP (ie size limitations and length of time)?
35) Are systems and storage dedicated to a particular client or is the system shared between multiple clients?
36) In order to meet policy obligations, OSFI’s data must remain only in Canada and cannot be stored or backed up elsewhere. Are MSSPs capable of meeting this requirement? How can OSFI get assurance this requirement is being met throughout the duration of the contract?

Technology and Trends

37) Is it typical that the client would have read-only remote access to client-owned log data on MSSP systems to allow for incident management or is access restricted to MSSP service staff only?
38) What client–owned systems would an MSSP typically integrate with?
39) Where would the technology required as part of this contract reside (client facilities or MSSP facilities)?
40) Will your services require the use of proprietary technology that OSFI must purchase or install? If so, please list all pertinent information related to this technology, including hardware, software, networking, middleware and database requirements.
41) Does the MSSP typically permit the sending of duplicate logs to both MSSP and client systems (ie. a SIEM or other log server on the client site)?
42) What are your top technology investment areas for a SOC today?
43) What bleeding edge technology investment will be relevant within the next 5 years for a SOC?
44) What new techniques are being employed by MSSPs to detect and respond to APTs?

Other Comments

45) Can you offer any other comments or recommendations which would help us plan/prepare for the potential RFP or outsourcing our SOC?