Request for Information

Title: Migration of DOC Cybersecurity Operations to the Cloud

Description:
The Department of Commerce (DOC) requires the ability to efficiently migrate and manage the applications and capabilities of its Enterprise Security Operations Center (ESOC), its Enterprise Cybersecurity Monitoring and Operations (ECMO), and its Continuous Diagnostic and Mitigation (CDM) program to a secure, FedRAMP-approved high (FIPS 199) impact level cloud service provider on an ongoing basis. This acquisition will consolidate the functionality and capabilities of these programs under unified management within the DOC OCIO organization. Because of the critical nature of these applications, DOC requires full operational capability of all services during the phased migration process.

Objective:
The objective of this Request for Information (RFI) is to gather information on the capabilities of existing FedRAMP-approved high impact level cloud service providers (CSPs) and their vendor-partners' experience migrating mission-critical applications (in this case, cybersecurity applications and capabilities) to the cloud on behalf of federal agencies.

Solution Overview:

DOC envisions that a potential contractor would perform the following:

1. Analyze DOC's current hosting environment(s) to determine its current cybersecurity operations infrastructure operating requirements;
2. Recommend a cloud hosting architecture, considering DOC's current and future cybersecurity operations capabilities;
3. Develop a project plan and oversee the migration of DOC's cybersecurity applications and operations to the federal cloud in consultation with DOC;
4. Procure and manage a highly flexible, scalable, secure, and available FedRAMP-approved high impact level cloud service provider on behalf of DOC;
5. Perform all necessary system security assessment and authorization (A&A) activities in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), National Institute for Standards and Technology (NIST) Special Publications, and DOC Information Technology Security Program Policy (ITSPP), Commerce Information Technology Requirements (CITR), and DOC Policy Memos;
6. Collect all information required to conduct a supply chain risk assessment;
7. Provide on-going maintenance and administration of the cloud hosting service;
8. Assist DOC in development of a service level agreement (SLA) and appropriate metrics for cloud hosting availability, operations management, and cost efficiency.

The DOC invites qualified and interested parties to submit written responses to this RFI by **July 31, 2017**, after which the DOC will review submitted materials to support the development of its RFP and acquisition strategy. All responses shall be limited to fifteen pages in length in addition to the general response requests included in Appendix A. Submitted responses will not be returned to the responding

party.

This RFI solicits information solely for market research purposes. As such, it does not constitute a Request for Proposal (RFP) or a commitment to issue an RFP by the DOC. The information provided by the responding party will neither be evaluated nor considered as an offer. This RFI does not commit the DOC to contract for any supply or service. Additionally, the DOC is not responsible for any administrative costs incurred by any responding party in response to this RFI.

Background:

Currently, DOC's ESOC and ECMO programs are hosted and overseen by staff at two separate component bureau locations – ESOC at NOAA in Fairmont, WV and ECMO at NIST in Germantown, MD. Because these locations and staff have bureau-related responsibilities and priorities, they are not solely dedicated to responding to DOC project/change requests and are not able to permit DOC staff to make changes to their environment. This has resulted in delays in configuration requests and in implementing new functionality. Additionally, bandwidth adequacy and scalability has impacted the ESOC's capacity to quickly and efficiently analyze transmitted log data.

DOC's continuing diagnostic and mitigation (CDM) program is currently funded by DHS. However, beginning in 2018, DOC will be required to begin funding components of this service and is considering migrating at least some if its storage and computing requirements to the cloud.

To improve DOC OCIO's access and ability to make timely changes to its cybersecurity monitoring environment, DOC OCIO seeks to migrate its existing ESOC/ECMO, and some parts of its CDM toolsets to a FedRAMP-approved high impact level cloud service provider. The cloud hosting environment would have the flexibility to easily scale in order to accommodate additional functionality and data log feeds as needed, and would offer a transparent pricing model to make costs predictable.

Current DOC Cybersecurity Infrastructure Components:

A. <u>DOC Enterprise Security Operations Center (ESOC)</u>

Co-located with NOAA's SOC in Fairmont, WV, the DOC Enterprise Security Operations Center (ESOC) has been designated as the Principal SOC for Commerce and is responsible for coordinating communication with DHS, US-CERT, OMB, and other Federal agencies. ESOC has established a sophisticated cyber security infrastructure that provides enterprise security event correlation and analysis, threat intelligence ingest, web vulnerability detection, malware IDS/IPS alert integration, and an automated security system for enterprise incident management and reporting.

In addition to these services, ESOC provides compliance for the NIST PM-16 control of implementing a cross-organization threat awareness program. ESOC satisfies this control by maintaining a Commerce Threat Intelligence Portal (CTIP) for collecting and distributing threat intelligence and cyber security information to the Commerce security user community.

ESOC is comprised of two primary components: Cyber Analytics and Incident Response. Each component is responsible for the following principal functions:

1. Cyber Analytics
   - Log Collection (establishing the logging environment from log source to centralized SIEM)
   - Threat Intelligence Harvesting and Curation (applying fidelity, confidence, and relevance values to ingested intelligence)
   - Enterprise Event Correlation (applying correlation logic against ingested security logs for analysis and investigation).
   - Intelligence and Awareness Sharing (distributing cyber intelligence to the constituency through the intelligence portal)
   - Log review/log analysis

2. Incident Response
   - Incident Handling (Collecting the information from the reporting entity (CA or reporting Bureau), identifying the necessary/applicable information)
   - Incident Processing (Triaging the incident, routing the incident to the appropriate department)
   - Incident Reporting (Reporting to external agencies, communicating applicable CCIRs, coordinating updates and closures)
   - Incident Investigation (Malware analysis, data forensics, additional dataset collection)

Applications Currently Utilized in DOC ESOC:

1. RSA Archer –
2. FireEye –.
3. ArcSight – Currently logging more than 3 billion events per week; this number will continue to grow as we begin to collect more data feeds from bureaus.
4. Web Inspect –
5. Encase --

B. **DOC ECMO Program**:

The Enterprise Cybersecurity Monitoring and Operations (ECMO) Program is a critical element of the CIO Cyber Security strategy for the US Department of Commerce. The ECMO Program fulfills the OMB requirement to continuously monitor security-related information from across the enterprise. ECMO provides essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO also provides performance metrics to support the administration's priority performance areas for continuous monitoring: automated asset management, automated configuration management and automated vulnerability management. The ECMO environment hosted at NIST was recently upgraded for higher performance, enhanced scalability, and support of additional security controls in order to accommodate all FIPS-199 High-Impact Systems owned by DOC.

Applications Currently Utilized in DOC ECMO:

1. **BigFix** – The Department of Commerce (DoC) currently utilizes IBM BigFix version 9.4 software within its ECMO to allow individual bureaus to perform cybersecurity monitoring as well as activities such as application and operating system patching. There are currently around 125,000 endpoints reporting. Due to latency issues, however, DOC has had to dramatically increase its processing power to provide its customer bureaus with acceptable performance. The ability to easily and cost effectively scale up or down to accommodate additional demand and/or incorporate additional functionality is desirable.

C. **Continuous Diagnostic and Mitigation (CDM) Program**:

The Department of Homeland Security's (DHS) Continuing Diagnostics and Mitigation (CDM) Program is a DHS mandated program. CDM provides federal agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Information feeds into bureau, agency, and federal level dashboards to provide situational awareness into cybersecurity risk posture across the agency and federal government.

The DHS CDM Program is being deployed in three (3) Phases:

- Phase I - (In process) – scheduled to be funded by DOC in FY2018
  - Hardware Asset Management (HWAM)
  - Software Asset Management (SWAM)
  - Vulnerability Management (VM)
  - Configurations Management (CM)
  - **Tools**:
    - IBM BigFix
    - Tenable Security Center
    - Continuous View
    - RES
    - Splunk
    - Archer Dashboard
- Phase II – (In design phase) – scheduled to be funded by DOC in FY2020
  - Credential Management (CRED)
  - Privileged Management (PRIV)
  - Tools:
    - Physical VMWare OVA AWS AMI
    - SailPoint as repository
    - Xceedium as Privileged Access Management Solution
    - Splunk for logging and auditing
- Phase III -- Includes boundary protection, event management and other capabilities TBD. Status: Pre-acquisition.

Information Requested:

1. Please complete the requested information using the response tables in Appendix A detailing your organization's profile (e.g. general, company, active/live client information, etc.).
2. What is the feasibility of the solution detailed in the Solution Overview section? Please consider security measures (e.g., FedRAMP, Trusted Internet Connections (TIC), etc.), scaling, and overall interoperability.
    a. What are the risks and considerations for the overall solution?
        i. If necessary, please detail potential alternatives that can successfully substitute the solution highlighted in this RFI.
3. What is the feasibility for a single vendor to orchestrate the provision of a cloud hosting provider, carry out the migration of existing ESOC/ECMO/CDM capabilities and conduct A&A services listed within the Capability Statements section of this RFI?
    a. What are the opportunities and limitations of that strategy?
        i. Please detail any recommended contract vehicles and acquisition considerations.
4. Please provide a rough order of magnitude (ROM) for the cloud hosting components you would consider using and the migration and A&A service components.
5. Please provide types and approximate number of personnel required to design, oversee migration, manage the environment day-to-day and close out the work listed in the solution overview over the first two years.
6. What information would you need to efficiently describe and price the appropriate solution in an RFP?
7. Does the proposed CSP solution provide an audit trail of which users perform which actions?
8. What is the CSP's role in the protection of the Departments data? What is the Department's (DOC's) role?
9. Are all data transmissions encrypted?
10. What access will be provided to logs from resources hosted?
11. What is your termination process for ensuring successful transition from your services to an alternative solution should the agreement end?
    a. How will the cloud service provider assist with the transition, including returning DOC's data in an effective manner?
    b. What are the provider's destruction or electronic shredding policies to insure DOC's data is no longer resident on the provider's systems and, therefore, not subject to attack or e-discovery?
    c. Does the provider have independent third parties that review and certify the efficacy of their exit procedures?
12. Where do the servers, processes, and data physically reside?
13. Who will be allowed to view DOC's data in the cloud?
14. What is cloud service provider's SLA for uptime?
15. Does the CSP allow customers to perform scheduled penetration tests of either the production environment or a designated testing environment?
16. How much control do DOC administrators have over DOC data?
17. How do you isolate and safeguard DOC data from that of other clients?
18. How does the cloud provider manage network and information security risks related to the cloud service?

19. Which security tasks are carried out by the provider, which type of security incidents are mitigated by the provider (and which tasks and incidents remain under the responsibility of the customer)?
20. How does the cloud service sustain disasters affecting data centers or connections, and how/where is data is backed up?
21. How is security of the cloud service guaranteed when there are legal issues or administrative disputes?
22. How is customer data or processes protected from unauthorized physical and logical access?
23. How does the cloud provider ensure software security and determine which software remains customer's responsibility?
24. How is access to the GUI's and API's protected, and are there additional measures for administrators/high privilege roles (under the customer's side)?
25. How is increase of usage or peaks handled, and what are the corresponding costs?
26. How do you screen your employees or contractors?
27. Does your solution rely on vendor-specific or product-specific capabilities which would hinder DOC from moving to another provider?

Respondents are required to limit their responses to fifteen pages, in addition to the requests in Appendix A, and should refrain from providing materials that are not relevant to this request (e.g. marketing materials).

Government Point of Contact (GPOC):
Please send responses to:

Anthony S. Kram
Contracting Officer
akram@doc.gov

and

Gordon C. Keller
Sr. Project Manager, DOC/OCIO/Office of Cybersecurity
gkeller@doc.gov
Email Subject Line: Request for Information – <*Insert Organization Name*>: DOC ESOC Migration to Cloud Initiative Response

Disclaimer and Important Notes:
Any organization responding to this notice should ensure that its response is complete and sufficiently detailed to allow the Government to determine the organization's qualifications to perform the work. Respondents are advised that the Government has no obligation to acknowledge receipt of the information received or provide feedback to respondents with respect to any information submitted. After a review of the responses received, a pre-solicitation synopsis and solicitation may be published.

Confidentiality:
No proprietary, classified, confidential, or sensitive information should be included in your response. The Government reserves the right to use any non-proprietary technical information in any resultant

solicitation(s).

Appendix A – General Response Tables

Organization Profile

General	Vendor Response
Company name.	
Address.	
City.	
State.	
Zip.	
Country.	
Primary Contact.	
Title.	
Phone.	

Company	Vendor Response
Number of years in business overall.	
Location of corporate and administrative services.	
Applicable Federal Certifications.	
Number of employees.	
Current / former federal clients for which your company has performed a cloud migration(s).	