Information Security Continuous Monitoring Capability Request For Information (RFI)

Solicitation Number: HSHQDC-11-Q-00021

Agency: Department of Homeland Security
Office: Office of the Chief Procurement Officer
Location: Office of Procurement Operations

Notice Type:
Sources Sought

Original Posted Date:
December 8, 2010

Posted Date:
December 9, 2010

Response Date:
Dec 22, 2010 10:00 pm Eastern

Original Response Date:
Dec 22, 2010 10:00 pm Eastern

Archiving Policy:
Automatic, 15 days after response date

Original Archive Date:
January 6, 2011

Archive Date:
January 6, 2011

Original Set Aside:
N/A

Set Aside:
N/A

Classification Code:
70 -- General purpose information technology equipment

NAICS Code:
423 -- Merchant Wholesalers, Durable Goods/423430 -- Computer and Computer Peripheral Equipment and Software Merchant Wholesalers

---

Synopsis:
Added: Dec 08, 2010 8:50 am Modified: Dec 09, 2010 10:47 am Track Changes
Information Security
Continuous Monitoring Capability
Request For Information (RFI)
Solicitation Number: HSHQDC-11-Q-00021
Notice Type: Sources Sought

Description:

Department of Homeland Security (DHS) is performing market research to determine industry interest and capabilities for information security continuous monitoring solutions. This is a Request for Information (RFI) announcement only. This is not a solicitation or request for proposal and in no way commits the Government to award a contract. DHS welcomes any and all constructive feedback/comments regarding this RFI.

DHS is interested in identifying candidate solutions that may address one or more of the capabilities required by the Department to implement information security continuous monitoring and risk reporting. Based on the general requirements and technical capabilities, DHS is interested in identifying the information security continuous monitoring solutions and technical requirements which reflect industry best practices.

General Requirements

• Solutions must be capable of being implemented across a range of computing environments to include:
  o Diverse network domains, in which an enterprise is composed of multiple networked domains that may or may not have trusted relationships
  o Geographically diverse networks, in which a geographically-diverse enterprise that is interconnected through networks may or may not have sufficient bandwidth to support continuous monitoring
  o Disconnected computing assets, assets that are disconnected from an agency's enterprise even though the agency has to account for them (e.g. laptops, mobile devices)
• Solutions must be scalable to a large agency with approximately 500,000 assets and capable of scaling to manage an estimated 600,000 events per second.
• Solutions must define and operate in a near real-time manner. However, capabilities to support manual data integration and disconnected computing assets should be described.
• Support National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) where applicable.
• Solutions should address capabilities and limitations associated with virtual computing platforms.
• Solutions should address the need for both connected and disconnected update capabilities. The solution may need to operate in both a classified and unclassified environment. Within a classified environment, automated updates will not be available from the Internet.

Continuous Monitoring Capabilities

The following automated capabilities are desired by the Department. Industry solutions may address one or more of the following capabilities.

1. Hardware asset inventory discovery, monitoring, and management.
  a. Hardware includes any information technology assets. For example, servers, workstations, laptops, mobile device, network devices and appliances.
2. Software asset inventory discovery, monitoring, and management.
3. Hardware and software configuration management.
  a. Include support for security configuration settings specified by the United States Government Configuration Baseline (USGCB)
4. Patch management.
5. Vulnerability assessment and remediation.
  a. Capable to access the latest version of security benchmarks from external sources, e.g. National Vulnerability Database (NVD).

6. Malware protection.
7. Data loss prevention (DLP).
8. Security incident and event management (SIEM).
9. Log aggregation within a federated organization.
10. Performance reporting.

General Instructions:

1. The Request for Information response shall include the following.
  a. Response to general requirements. Limit 4-pages.
  b. Statement describing how the proposed solution meets each continuous monitoring capability. Limit 3-pages per capability addressed.
  c. List the requirements for information security continuous monitoring that the submitter believes are addressed by the proposed solution. The requirements should reflect the unique capabilities or functions that that the solution provides in order to manage information security risk in a near real-time manner. Limit 5-pages per capability.
  d. Describe any recommended metrics the solution would enable the Department to address. Identify the type of metric (implementation, effectiveness/efficiency, or impact) as defined in NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security. Limit 3 pages per capability.
  e. The Department of Homeland Security is interested in mature/developed solutions. Respondents shall provide information on previous deployments of the respondents' solution, and may include both government and commercial deployments that the respondent has performed. Include customer names and addresses, description of work performed/delivered, description of types/complexity of systems worked on, and description of strategies to accomplish the work. Limit your response to five (5) pages.
  f. Feedback and/or comments in regards to this RFI (optional). Limit three (3) pages.
2. Sales brochures, videos, and other marketing information materials are not solicited and will not be reviewed.
3. Do not submit cost or price information with the response.
4. Interested parties shall submit an electronic copy of their responses via email to: Contract Specialist, Sharee Richardson; Sharee.Richardson@DHS.Gov. The due date and time for submission of responses is Wednesday, December 22, 2010 at 10:00 PM Eastern Standard Time.
5. No phone calls related to this Request for Information will be accepted. All correspondence shall be via email.
6. Any proprietary information contained in the response must be marked accordingly.
7. Respondents are solely responsible for expenses associated with this RFI.
8. Respondents will not be notified of the results of the review.
9. Respondents shall include their DUNS number and GSA Schedule Contract Number or GSA Government-wide Acquisition Contract Family and Number if applicable.

Respondents should note that this RFI is being issued solely for information and planning purposes and does not constitute an Invitation for Bids (IFB), a request for Proposals (RFP), a Request for Quotation or an indication that the Government will contract for any items and/or services contained in this notice. All information received in response to this notice that is marked ‘Proprietary' will be handled accordingly. Responses to this notice will not be returned. In submitting a response, you are solely responsible and accountable for all of the expenses associated with your response. The following provision(s) is applicable to this notice and is hereby incorporated by reference: FAR 52.215-3 Request for Information or Solicitation for Planning Purposes (Oct 1997) The full text of this clause is available at: http://www.aqcuisition.gov/far/index.html

Contracting Office Address:
Office of the Chief Procurement Officer
Washington, District of Columbia 20528
United States

Place of Performance:
Washington, District of Columbia 20024
United States

Primary Point of Contact.:
Sharee L. Richardson,
Contract Specialist
sharee.richardson@dhs.gov
Phone: 202-447-0624
Fax: 202-447-5564

Secondary Point of Contact:
Andrew H. Cole,
Contracting Officer
andrew.h.cole@hq.dhs.gov
Phone: 202-447-5586
Fax: 202-447-5564

Opportunity History

- Original Synopsis
  Sources Sought
  Dec 08, 2010
  8:50 am
- Changed
  Dec 09, 2010
  10:48 am