Continuous Monitoring Program Stalled, New Policy Forthcoming

Posted At : October 16, 2013 10:48 AM | Posted By : Kyra Fussell

Related Categories: Department of Homeland Security, Office of Management and Budget, Events, Information Security, Cybersecurity, Policy & Legislation, General Services Administration (GSA)

In August 2013, the Department of Homeland Security (DHS) issued awards to seventeen vendors for a potential $6 billion contract to support a government-wide network threat monitoring program. On the heels of those announcements, the program implementation faced hurdles around legislation and budget. While progress seems to have been stalled during the shutdown, the Office of Management and Budget (OMB) is preparing to issue new policy providing direction to agencies on implementing federal information system continuous monitoring (FISCM).

Part of a massive effort, DHS's Continuous Diagnostic and Mitigation (CDM) program will provide information technology tools and continuous monitoring as a services (CMaaS) to combat threats on government civilian networks. The program aims to establish a common set of tools and services in place aligned with national and industry standards. These capabilities would enable agencies to be more responsive to network anomalies.

The core capabilities for DHS's continuous monitoring fell into five areas: hardware asset management, software asset management, vulnerability management, configuration management, and anti-virus. The continuous monitoring program outlined several approaches, including a service-based solution. These CMaaS solutions will be based upon NIST standards including a number of guidelines set out in NIST's 800 series of **special publications**.

Source: GSA

DHS received $183 million from Congress in 2013 to support financing this effort for many agencies. **Although Blanket Purchase Agreements (BPAs) were awarded out of DHS's Office of Cybersecurity and Communications Continuous Diagnostics and Mitigation Program**, the contracts will be run by the General Services Administration (GSA). Earlier this month, the momentum reportedly stalled. Vendors expecting the release of a request for quote (RFQ) under the contract last week are continuing to wait for further action. The RFQ was expected to address agencies' requirements for information technology inventory management tools for both hardware and software.

In the meantime, new information security policy from OMB is in the works to clarify the types of systems and data that are monitored. **Recent reports** suggest that the policy has been ready for a few weeks but officials have withheld the release pending further review. At over ten pages, the policy is expected to offer comprehensive guidance for federal information system continuous monitoring (FISCM).

Amid numerous recent cancellations of government events, an upcoming CDM workshop was announced. Scheduled for November 6, 2013, **the event** will explore threats to federal systems, leveraging diagnostics and monitoring to improve information security, as well as use cases and examples.

*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWinIQ**. Follow me on Twitter **@FIAGovWin**.*