Energy Department Cloud Services Need Oversight

Posted At : October 7, 2014 9:45 AM | Posted By : Kyra Fussell
Related Categories: Department of Agriculture, Department of Defense, Department of Homeland Security, Office of Management and Budget, Information Security, Cloud Computing, Department of Energy, Cybersecurity, Department of Commerce

In September 2014, the Department of Energy's (DOE) Inspector General (IG) released findings from an audit of the cloud environments across DOE. The report highlighted several issues including problems with inventory management and implementation of security controls. These problems were linked to a more fundamental concern: DOE lacks a cloud strategy.

The DOE issues around cloud inventorying practices are reminiscent of challenges agencies encountered when taking stock of data centers and software applications. Lack of visibility and transparency raise difficulties around duplication of effort and ensuring return on investment for cloud services. DOE estimates that spending on independently acquired and managed cloud services are in excess of $30 million.

Reviews of eight contracts provided at six different locations determined that the contract did not properly or consistently address business and cybersecurity risks. The inconsistent implementation of security controls raises serious compliance issues with internal guidance as well as with the Federal Risk and Authorization Management Program (FedRAMP). The DOE cloud program audit found inconsistent and incomplete compliance with FedRAMP, which agencies were supposed to achieve by June 2014. More troublesome than having some programs in process of implementing requirement was the fact that DOE had erroneously reported to the Office of Management and Budget (OMB) that the majority of DOE cloud services met all FedRAMP requirements.

Departmental management concurred with the IG's recommendations, including the need to establish an enterprise approach to implementation of cloud computing and to ensure oversight of adoption efforts. The FY 2014-2018 DOE Information Resource Management (IRM) Strategic Plan replaces over 15 different strategic documents and efforts. One of the objectives outlined in the IRM document calls out a target for creating a network of the department's clouds, which may serve as a high level strategy. DOE plan to update its departmental cyber security program (DOE Order (O) 205.1B) to include clear requirements and guidance around oversight of cloud computing efforts. DOE is also in discussions with the FedRAMP program management office to evaluate DOE-specific FedRAMP requirements that would be included in the revision of DOE O 205.1 B. As for the issues around contracting inconsistencies, DOE expects to continue working on contracting guidance and standard clauses as well as leveraging work with the Federal CIO Council to identify and adopt best practices. All of the recommendations share the same estimated completion date of September 30, 2015.

DOE's IG attributes some of these issues to the lack of a comprehensive cloud strategy. For example, the inventory of cloud initiatives was incomplete. DOE reported only 44 ongoing initiatives to OMB. Review found, however, that DOE has at least 130 initiatives across 24 federal and contractor locations. An overarching strategy would have provided a foundation for coordination of efforts along with oversight and risk management.

It's fair to expect more reports on cloud implementation practices from other agencies to follow, since this DOE audit links back to a NASA audit and a government-wide review. In July 2013 NASA's IG published a report that found the agency lacked governance to support efficient cloud implementation. According to the DOE audit, "As a result of issues identified during [the NASA IG cloud program] audit, a Government-wide initiative was undertaken by the Council of Inspectors General for Integrity and Efficiency to provide insight to agency heads and lawmakers on how well the Federal government has adopted cloud computing technologies. In support of that effort, [the Energy Department] initiated this audit to determine whether the Department efficiently and effectively managed its cloud computing environment."

Historically, some agency reporting has fallen under other IT areas, like security. For example, USDA's audit of the department's information security included review of cloud services. Similar to the findings of the DOE audit, the USDA **report** highlighted hurdles around contracting and managing risks. **Another instance** comes from the Department of Homeland Security (DHS).

More recently, however, reports have singled out cloud computing adoption as a focus. At the start of 2014, the Transportation Department **announced** it was auditing practices for acquiring and monitoring cloud services. In July of this year, the EPA **released findings** from its review of cloud technology adoption. Other

agencies have announced or planned audits that are likely still in the works. Last December, for example, the Commerce Department **announced** that it had commenced an audit of cloud-computing environments. As part of the planned projects around cybersecurity, **Department of Defense's IG audit plan for FY 2014** included evaluating the efficiency of their cloud migration strategy and efforts. With a number of reports still underway, it's too soon to fully assess how the government has fared in its adoption of cloud computing. So far, however, issues around governance, oversight and risk management appear to be thematic.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@FIAGovWin** .*