Will the Defense Inspector General Further Delay the DoD's Migration to the Cloud?

Posted At : December 16, 2014 10:31 AM | Posted By : Alex Rossino
Related Categories: Department of Defense, Technology Trends, Cloud Computing, Federal, Emerging Technologies

Recently, the Department of Defense's Office of the Inspector General **published an audit report** critical of the department's efforts to implement its 2012 cloud computing strategy. Citing material weaknesses in the execution of the strategy, including the failure to adequately train acquisition personnel who procure cloud services, the failure to fully develop cloud service broker management capabilities, the failure of DoD components to obtain proper waivers from review authorities to use non-DoD approved clouds, and the failure of the DoD CIO to develop a detailed written process for obtaining a cloud computing waiver, the OIG concluded that the department had put data at risk while also not reaping the cost savings benefits that cloud computing offers.

The DoDIG report is the latest in a series of similar reports from other government agencies that also revealed systematic flaws in efforts to leverage cloud computing. Taken together, these audit reports point to the disruption that cloud computing is causing in federal agency information technology environments. This disruption is not necessarily related to technology difficulties, although these are a concern. Rather, it is related to weaknesses in the policy and governance processes that guide agency IT investments. Cloud computing is creating challenges that agencies simply aren't equipped to handle, a problem made worse by policies like Cloud First, which has forced agencies to dive into a technology for which they aren't prepared.

In the DoD's case, the lack of policy and governance oversight is particularly perplexing considering the glacial pace at which the Defense Department has moved toward using commercial cloud solutions. The DoDIG's audit now threatens to bring that progress to a halt as the DoD CIO and defense components consider how to respond to the OIG's recommendations. A real question at this point is should they bother to respond at all. Several elements of the OIG report are based on assumptions and policies that have changed considerably since the DoD Cloud Computing Strategy was released in June 2012. Take, for example, cloud brokering, which acting DoD CIO, Terry Halvorsen, has de-centralized. In addition to the Cloud Brokerage Project Management Office at the Defense Information Systems Agency there are now cloud brokerages at the Army's Program Executive Office Enterprise Information Systems and the Navy's Space and Naval Warfare Systems Command.

Similarly, the DoDIG castigates the department for failing to implement an enterprise contract for commercial cloud services. The goal of implementing an enterprise contract, however, no longer resembles the reality of the situation at the DoD. When acting CIO Halvorsen gave the Services the ability to procure commercial cloud services he effectively eliminated the need for an enterprise level cloud contract. In other words, the DoDIG calls the DoD CIO to account for not implementing an irrelevant procurement strategy.

None of this is to say that the DoD has somehow miraculously solved its challenges. There is indeed a pressing need for acquisition training and contract clauses that will ensure a proper level of cloud service and data security. Similarly, if it is to be retained, the waiver process needs to be improved. In itself, it is unclear if waivers will be necessary given DISA's enhanced role as certifier of cyber security requirements for commercial providers. DISA's imprimatur is effectively a waiver, if the commercial solution meets security requirements.

Improvements are needed, but one wonders if it is not a counter-productive use of time for the DoD CIO, DISA, and the Services to spend time addressing a critique that does not fit current conditions. The implementation of the Joint Information Environment addresses the use of commercial cloud solutions in a way that should assuage the cyber security concerns of the DoDIG. Furthermore, the de-centralization of cloud procurement is intended to eliminate the acquisition bottleneck at the DISA Cloud PMO while also reducing costs. These are solid steps toward removing barriers to commercial cloud use at the DoD. Will they be allowed to bear fruit or will they be suffocated by the weight of adherence to outdated policy demands?