Department of Veterans Affairs

Memorandum

Date: January 14, 2013

From: Deputy Assistant Secretary, Information Security

Subj: System Authority to Operate Concern

To: Assistant Secretary, Information and Technology

As the Deputy Assistant Secretary for Information Security (DAS) and Department Chief Information Security Officer (CISO), I'd like to raise a concern regarding the process to complete Authority to Operate (ATO) extension activities for approximately 545 systems in the VA inventory during the month of January 2013; and also raise issue with the Department engaging in a low value, static and sun setting ATO process in any way, shape or form, that is diametrically contrary to the way the US government requires Departments and Agencies to manage system risks.

Issue

In 2011, the Office of Information Security (OIS) recommended to the Assistant Secretary for Information and Technology to extend the ATOs for all systems with an imminent expiration date for 16 months. During the extension period, it was the intent of OIS, consistent with Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), to move all VA information systems into a continuous diagnostics/monitoring and remediation program. The continuous diagnostic and remediation program is consistent with National Institute of Standards and Technology (NIST) guidance and is intended to position VA's information systems security program as a proactive one, which allows for the monitoring and remediation of system risk in a near real time manner.

In the move away from the static processes leading to an ATO, OIS encountered delays with the implementation of the continuous diagnostic/monitoring program, most notably with the deployment of the underlying governance, risk and compliance (GRC) subsystem, delays that lead to the termination of the implementing vendor's contract. The length of time it took to terminate the contract coupled with the time it took to establish a contract to acquire a new GRC tool resulted in the expiration of the 545 ATOs before they could be rolled into the newly acquired GRC tool.

As a result of this, it was recommended to the Principal Deputy Assistant Secretary, OIT (PDAS) that all 545 system ATOs be extended until August 31, 2013, which will allow sufficient time to deploy the new GRC tool and populate the tool with system information for near real time diagnostics and remediation. This would allow for VA to focus on meeting the metrics established by OMB and DHS for continuous diagnostics and provide a much better assurance of system security posture. These same metrics are being used in 2013 by the VA Office of Inspector General (OIG) as part of their 2013 Federal Information Security Management Act (FISMA) audit of VA's system.

We currently have a requirement by the PDAS to conduct a myriad of static and low value activities against the 545 systems and present the extension packages to the Designating Approving Authority (DAA) for signature. These activities are contrary to the path required by OMB and DHS for identifying and managing system risks. Furthermore, on Thursday January 11th it was made the requirement of the PDAS that all activities for all 545 systems be

completed by January 25th, 2013, which is the final day of tenure for the Department's DAS, Information Security as CISO.

Concern

As DAS, IT Security and the Department's CISO I have three primary concerns:

1. Attempting to prosecute these activities using an expedited process is extremely risky. There undoubtedly will be errors and omissions in process and procedures in the rush to complete these activities. I cannot and will not sign as the DAS, Information Security any artifact attesting positively to a process that does not add value, is not needed, is wasteful, unnecessarily uses up resources and jeopardizes the integrity of the information security program. I would also recommend that the DAA not sign or attest to any artifact resulting from this abbreviated and expedited activity.
2. The activities that are required to extend ATOs are in opposition to the direction that VA needs to execute in order to reach the goal of CDR as required by OMB and DHS. The current process will further set VA behind in reaching stated goals.
3. By not moving out in an expeditious fashion in the goal to establish a CDR program in 2013, VA will be deficient in key metrics evaluated and reported on to Congress by OMB, DHS and the VA OIG. The OIG intends to evaluate VA's implementation of CDR during 2013, instead of the old static processes previously employed by VA in support of system gaining system ATOs.

Remediation

To remedy this issue, I have three recommendations:

1. Stop moving forward with the activities to extend the ATOs. The ATO's are largely expired and the expedited process required for another extension is unnecessary and does not provide any measurable value nor do they increase system security.
2. Establish a memorandum for the file which stipulates; as system ATOs expire, those systems will be rolled into the CDR program as quickly and soundly as possible. This is consistent with the direction required by both OMB and DHS for managing system security in a proactive and near real time fashion. It is also what the OIG expects to see as they begin the review the Department's CDR program as part of their 2013 FISMA audit activity.
3. Focus any expedited processes on the implementation of the CDR program and the underlying GRC tools and begin to roll systems into the GRC platform in accordance with the prescribed project schedule.

Jerry L. Davis