GAO Highlights

Highlights of GAO-15-220T, a testimony before the Committee on Veterans' Affairs, House of Representatives

November 18, 2014

INFORMATION SECURITY

Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk

Why GAO Did This Study

VA relies extensively on information technology systems that collect, process, and store veterans' sensitive personal information. Without adequate safeguards, these systems and information are vulnerable to compromise. Further, VA has faced long-standing challenges in securing its systems, and reported incidents have demonstrated the impact of cyber-based threats on the confidentiality, integrity, and availability of veterans' personal information.

This statement summarizes GAO's November 13, 2014, report on VA efforts to address previously identified information security vulnerabilities. For its review, GAO focused on efforts to respond to a network intrusion, address vulnerabilities in key web-based applications, and remediate weaknesses in devices connected to the department's network. To conduct its work, GAO reviewed the results of VA security testing; interviewed department officials; and reviewed policies, procedures, and other documentation.

What GAO Recommends

In its report, GAO made eight recommendations to VA to fully address weaknesses in incident response, web applications, and patch management. VA concurred with GAO's recommendations.

What GAO Found

The Department of Veterans Affairs (VA) has taken actions to mitigate previously identified vulnerabilities, but it has not fully addressed these weaknesses:

- **Incident response:** VA took actions to contain and eradicate the effects of a network intrusion detected in 2012, but it could not show that these actions were fully effective. Specifically, the department's Network and Security Operations Center (NSOC) analyzed the incident and documented actions taken in response, but the department could not provide forensics analysis or digital evidence associated with its efforts. Thus, the effectiveness of its incident response could not be demonstrated. VA policy does not require evidence related to security incidents to be kept for at least 3 years, as recommended by federal guidance. This hinders the department's ability to show its efforts have been effective. Further, VA did not fully address the vulnerability that led to the original incident, increasing the risk that such an incident may recur. In addition, VA policy does not provide the NSOC with sufficient authority to monitor activity on the department's networks, limiting its ability to detect and respond to security incidents.
- **Vulnerabilities in web applications:** VA's NSOC identified nine significant vulnerabilities in two key applications that process veterans' personal information, and validated that the department had corrected six of them. However, corrective actions for the remaining three vulnerabilities had not been validated, and the department had not developed action plans to ensure they were addressed in a timely manner. VA also did not fully implement a type of testing that can identify root causes of security vulnerabilities in application source code.
- **Weaknesses on network devices:** VA periodically scans the devices (e.g., laptop computers) connected to its network for security vulnerabilities and summarizes the most critical vulnerabilities. For May 2014, the 10 most critical vulnerabilities were related to security patches that had not been applied to VA's network devices. These missing patches had been available for periods ranging from 4 to 31 months, even though department policy requires critical patches to be applied within 30 days. While the department documented decisions not to apply 3 of the patches, pending tests of the effect they could have on functionality, it did not document controls to compensate for not applying up-to-date security features. Further, the department did not document any reasons for not applying the other 7 patches. The department has established an organization tasked with remediating security vulnerabilities, but it has not developed specific actions, priorities, and milestones for this organization to carry out its responsibilities.

Until VA fully addresses identified security weaknesses, its systems and the information they contain—including veterans' personal information—will be at an increased risk of unauthorized access, modification, disclosure, or loss.

View GAO-15-220T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.