United States Government Accountability Office

Testimony

Before the Committee on Veterans' Affairs, House of Representatives

INFORMATION SECURITY

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

Statement of Gregory C. Wilshusen, Director
Information Security Issues

GAO-15-220T

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.

_____ **United States Government Accountability Office**

Chairman Miller, Ranking Member Michaud, and Members of the Committee:

Thank you for inviting me to testify at today's hearing on information security weaknesses at the Department of Veterans Affairs (VA). Securing its information and systems is particularly critical for VA because its mission of promoting the health, welfare, and dignity of our nation's veterans requires it to collect and maintain sensitive personal information in the course of, for example, providing medical care to veterans. While federal law, primarily the Federal Information Security Management Act of 2002 (FISMA),[1] requires federal agencies to implement an agency-wide information security program, protecting information and systems is a major challenge for the federal government. We first designated the protection of federal information systems as a government-wide high-risk area in 1997 and continued to do so in the most recent update to our high-risk series.[2]

As you know, VA has faced long-standing challenges in its efforts to secure its information and information systems. For example, as we have previously testified, VA has consistently had weaknesses in key information security control areas.[3] Moreover, reports of incidents affecting VA's systems highlight the serious impact that inadequate information security can have on the confidentiality, integrity, and availability of veterans' personal information. For instance, in January 2014, a software defect in a VA system used by veterans to access personal information and services allowed users to view the personal information of other veterans, potentially affecting 1,301 veterans or their dependents, according to a VA official.

My statement today will summarize the key findings from our November 13, 2014, report on VA's efforts to address previously identified information security vulnerabilities.[4] These weaknesses pertained

---

[1]FISMA was enacted as title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[2]GAO, *High-Risk Series: An Update,* GAO-13-283 (Washington, D.C.: Feb. 14, 2013).

[3]GAO, *Information Security: VA Needs to Address Long-Standing Challenges,* GAO-14-469T (Washington, D.C.: Mar. 25, 2014).

[4]GAO, *Information Security: VA Needs to Address Identified Vulnerabilities*, GAO-15-117 (Washington, D.C.: Nov. 13, 2014).

specifically to incident response efforts, vulnerabilities in key web applications,[5] and vulnerabilities in devices connected to VA's network.

To conduct our work, we reviewed the results of VA security testing; interviewed department officials; and reviewed policies, procedures, and other documentation. Further details on the objective, scope, and methodology of our review can be found in the report. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards.

VA Has Not Fully Addressed Previously Identified Security Vulnerabilities

VA has taken actions to mitigate previously identified vulnerabilities, but more needs to be done to fully address these weaknesses:

VA could not demonstrate that its response to a security incident was effective. VA's Network and Security Operations Center (NSOC) took actions to address an incident involving intrusions by "malicious outsiders" identified in 2012. For example, it had identified hosts it believed were affected by the intrusion and taken steps to eradicate the effects from those hosts. The NSOC also documented actions taken to address the incident to the point where staff believed it had been successfully remediated.

However, VA could not demonstrate the effectiveness of its efforts because staff could not locate the associated forensics analysis report or other key materials. Officials explained that digital evidence for incident response was only maintained for 30 days due to constraints on storage space. Subsequently, VA established a standard operating procedure requiring forensics analysis reports to be maintained for 6 years, but allowing the associated digital evidence to be purged after 1 month. This is inconsistent with federal guidance, which calls for records related to security-incident handling to be maintained for 3 years.[6] Without preserving such evidence, VA will be unable to demonstrate the effectiveness of its incident-response measures, and may be hindered in

---

[5]A web application is software that performs a specific function directly for a user, and is run on a web server (as opposed to a user's desktop) and accessed through a web browser.

[6]National Archives and Records Administration, *General Records Schedule 24: Information Technology Operations and Management Records*, Transmittal No. 22 (April 2010).

assisting law enforcement agencies in investigating and prosecuting cyber crimes.

Moreover, VA had not yet addressed the underlying vulnerability that allowed the 2012 incident to occur. The agency had planned to implement a solution in February 2014 that would have corrected the weakness, but this had not been completed at the time of our review. VA did limit access to the affected system, but this is insufficient to prevent recurrence of such an incident.

With respect to incident response more broadly, we found that the department's NSOC did not have sufficient visibility into VA's computer networks, limiting its ability to detect and respond to incidents. This is because VA policy does not define the NSOC's authority to access activity logs collected at VA data centers. We previously raised the issue of defining incident response roles and responsibilities at VA in an April 2014 report[7] and recommended that VA define the incident response team's level of authority. VA concurred with this recommendation. Implementing this recommendation should include providing the NSOC with authority to review network activity logs.

The NSOC is taking actions to improve its incident response capabilities, such as analyzing how best to restrict access to VA's network and planning to purchase new tools. However, it has not established a time frame for completing these actions.

VA did not fully address weaknesses in key web applications. VA's NSOC had identified eight high-risk vulnerabilities affecting two key web applications that process veterans' sensitive personal information, as well as a critical vulnerability in one of the applications related to the protection of personally identifiable information. As of June 2014, VA had corrected six of the nine vulnerabilities. For example, the department validated that the critical vulnerability involving personally identifiable information had been corrected within 1 week. However, the VA had not validated corrective actions taken for the other three. One of these vulnerabilities had been outstanding for over a year. Further, the department had not developed plans of action and milestones for addressing these

---

[7]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices,* GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

vulnerabilities, resulting in less assurance that they would be corrected in a timely and effective manner.

In addition, VA did not scan the software code in its web applications using "static analysis" tools, which can identify root causes of software security vulnerabilities.[8] Officials from VA's Office of Cybersecurity stated that the department had begun to use static analysis to conduct source code reviews in January 2013 and had drafted a policy requiring the use of such tools. But as of the time of our review, source code review was occurring for only one of the two applications we reviewed.

VA had not mitigated vulnerabilities in department workstations. VA periodically scans its network devices—predominantly workstations (for example, laptop computers)—for vulnerabilities that have been identified by software vendors. This is consistent with federal guidance and VA policy, which require periodic vulnerability scanning. Specifically, the NSOC scans workstations across the department's network at least monthly and summarizes the most critical vulnerabilities, such as those requiring patches to remediate them.

However, VA has not always addressed identified vulnerabilities in a timely fashion and consistent with department policy. That policy requires critical patches to be applied within 30 days or, in cases where patches cannot be applied or impact performance, the department is to develop compensating controls and/or plans to migrate to newer services that allow security patches and features to be applied. As of May 2014, the 10 most prevalent critical vulnerabilities identified by department scans were software patches that had not been applied. Regarding these missing patches,

- they had been available for periods ranging from 4 to 31 months;
- there were multiple occurrences of each missing patch, ranging from approximately 9,200 to 286,700; and
- each patch was intended to mitigate multiple vulnerabilities, ranging from 5 to 51, with a total of 301 vulnerabilities.

---

[8]Various tools, such as "static analysis" tools, can scan software source code, identify root causes of software security vulnerabilities, and correlate and prioritize results. The National Institute of Standards and Technology states that vulnerability analyses for custom software applications may require additional approaches, such as static analysis. This type of analysis can help developers identify and reduce or eliminate potential flaws.

While VA had decided not to apply the top three critical patches until testing could determine the effect they would have on various applications, this decision was made after the patches had been available for 3 to 10 months, exceeding the 30-day requirement for applying critical patches. Nor did the department describe compensating controls or plans to migrate to services that would support security features. For the other 7 patches, VA did not provide documentation of any decisions not to apply them.

In addition, scanning procedures VA uses may not identify certain vulnerabilities. Specifically, VA's scans of its non-Windows systems, such as Linux systems, were conducted in "unauthenticated" mode. This means that the scans did not test as a logged-in user of the systems, which would allow for the examination of additional security controls. Thus, vulnerabilities on these systems may go undetected.

VA has efforts under way to improve its vulnerability remediation. In May 2013 it established an organization tasked with overseeing processes for vulnerability remediation, among other things. Moreover, the organization has taken steps to carry out its responsibilities by, for example, planning to create a database to track remediation and patch implementation. However, the department has yet to establish specific actions, priorities, and milestones for the organization to carry out its tasks. Establishing such elements contributes to evaluating progress, achieving results, and ensuring effective oversight.

Implementing GAO's Recommendations Can Help VA Mitigate Weaknesses

In our report, we made eight recommendations to VA to address the previously identified security vulnerabilities:

- Update the department's standard operating procedure to require evidence associated with security incidents to be maintained for at least 3 years.
- Fully implement the solution to address the weakness that led to the 2012 intrusion.
- Establish time frames for completing planned actions to improve incident response.
- Develop plans of action and milestones to address critical and high-risk vulnerabilities in the two key web applications.
- Finalize and implement the policy requiring source code scans on key web applications.

- Apply missing security patches within established time frames or document compensating controls and/or plans to migrate to newer services that support security features.
- Scan non-Windows (e.g., Linux) network devices in authenticated mode.
- Identify actions, priorities, and milestones for tasks related to vulnerability remediation.

In comments on a draft of our report, VA stated that it generally agreed with our conclusions and concurred with our recommendations. VA also stated that it had already taken actions to address six of our eight recommendations and has plans in place to address the other two. However, we have not yet validated the actions described or determined whether they effectively address the issues raised in the report. Moreover, we are concerned that VA's described actions for two of the recommendations may not fully address the identified weaknesses. We intend to monitor VA's implementation of our recommendations.

In summary, while the department has taken steps to respond to incidents and identify and mitigate vulnerabilities, ensuring effective information security remains a challenge for VA. Shortcomings in its incident response activities, vulnerabilities in key web applications, and weaknesses in the management of security on its network devices place the sensitive personal information entrusted to the department at increased risk of unauthorized access, modification, disclosure, or loss. Our recommendations, if properly implemented, should help the department improve its security posture and better protect this information.

Chairman Miller, Ranking Member Michaud, and Members of the Committee, this concludes my statement. I would be pleased to answer any questions you may have.

Contact and Staff Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Other key contributors to this testimony include Jeffrey Knott, Lon Chin, Harold Lewis, and Chris Warweg (assistant directors); Jennifer R. Franks; Lee McCracken; and Tyler Mountjoy.