



Report to the Chairman, Committee on
Veterans' Affairs, House of
Representatives

November 2014

INFORMATION SECURITY

VA Needs to Address Identified Vulnerabilities

GAO Highlights

Highlights of [GAO-15-117](#), a report to the Chairman, Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

In carrying out its mission to ensure the health, welfare, and dignity of the nation's veterans, VA relies extensively on information technology systems that collect, process, and store veterans' sensitive information. Without adequate safeguards, these systems and information are vulnerable to a wide array of cyber-based threats. Moreover, VA has faced long-standing challenges in adequately securing its systems and information, and reports of recent incidents have highlighted the serious impact of inadequate information security on the confidentiality, integrity, and availability of veterans' personal information.

GAO was asked to review VA's efforts to address information security vulnerabilities. The objective for this work was to determine the extent to which selected, previously identified vulnerabilities continued to exist on VA computer systems. To do this, GAO reviewed VA actions taken to address previously identified vulnerabilities, including a significant network intrusion, vulnerabilities in two key web-based applications, and security weaknesses on devices connected to VA's network. GAO also reviewed the results of VA security testing; interviewed relevant officials and staff; and reviewed policies, procedures, and other documentation.

What GAO Recommends

GAO is making eight recommendations to VA to address identified weaknesses in incident response, web applications, and patch management. In commenting on a draft of this report, VA stated that it concurred with GAO's recommendations.

View [GAO-15-117](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

November 2014

INFORMATION SECURITY

VA Needs to Address Identified Vulnerabilities

What GAO Found

While the Department of Veterans Affairs (VA) has taken actions to mitigate previously identified vulnerabilities, it has not fully addressed these weaknesses. For example, VA took actions to contain and eradicate a significant incident detected in 2012 involving a network intrusion, but these actions were not fully effective:

- The department's Network and Security Operations Center (NSOC) analyzed the incident and documented actions taken in response. However, VA could not produce a report of its forensic analysis of the incident or the digital evidence collected during this analysis to show that the response had been effective. VA's procedures do not require all evidence related to security incidents to be kept for at least 3 years, as called for by federal guidance. As a result, VA cannot demonstrate the effectiveness of its incident response and may be hindered in assisting in related law enforcement activities.
- VA has not addressed an underlying vulnerability that allowed the incident to occur. Specifically, the department has taken some steps to limit access to the affected system, but, at the time of GAO's review, VA had not fully implemented a solution for correcting the associated weakness. Without fully addressing the weakness or applying compensating controls, increased risk exists that such an incident could recur.
- Further, VA's policies did not provide the NSOC with sufficient authority to access activity logs on VA's networks, hindering its ability to determine if incidents have been adequately addressed. In an April 2014 report, GAO recommended that VA revise its incident response policies to ensure the incident response team had adequate authority, and VA concurred.

Further, VA's actions to address vulnerabilities identified in two key web applications were insufficient. The NSOC identified vulnerabilities in these applications through testing conducted as part of the system authorization process, but VA did not develop plans of action and milestones for correcting the vulnerabilities, resulting in less assurance that these weaknesses would be corrected in a timely and effective manner.

Finally, vulnerabilities identified in VA's workstations (e.g., laptop computers) had not been corrected. Specifically, 10 critical software patches had been available for periods ranging from 4 to 31 months without being applied to workstations, even though VA policy requires critical patches to be applied within 30 days. There were multiple occurrences of each missing patch, ranging from about 9,200 to 286,700, and each patch was to address an average of 30 security vulnerabilities. VA decided not to apply 3 of the 10 patches until it could test their impact on its applications; however, it did not document compensating controls or plans to migrate to systems that support up-to-date security features. While the department has established an organization to improve its vulnerability remediation, it has yet to identify specific actions and milestones for carrying out related responsibilities. Until VA fully addresses previously identified security weaknesses, its information is at heightened risk of unauthorized access, modification, and disclosure and its systems at risk of disruption.

Contents

Letter		1
	Background	2
	Although VA Has Taken Mitigation Actions, Previously Identified Vulnerabilities Continue to Exist	6
	Conclusions	14
	Recommendations for Executive Action	14
	Agency Comments and Our Evaluation	15
Appendix I	Objective, Scope, and Methodology	17
Appendix II	Comments from the Department of Veterans Affairs	20
Appendix III	GAO Contacts and Staff Acknowledgments	25
Table		
	Table 1: Status of Critical and High-Risk Vulnerabilities Identified in Two Key VA Web Applications	10

Abbreviations

CIO	chief information officer
CISO	chief information security officer
FISMA	Federal Information Security Management Act of 2002
IT	information technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSOC	Network and Security Operations Center
OIG	Office of Inspector General
PII	personally identifiable information
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



November 13, 2014

The Honorable Jeff Miller
Chairman
Committee on Veterans' Affairs
House of Representatives

Dear Mr. Chairman:

In carrying out its mission of serving the nation's veterans, the Department of Veterans Affairs (VA) relies extensively on information technology (IT) systems to, among other things, collect, process, and maintain personal information on veterans. Protecting information and systems is a major challenge for the federal government, and both GAO and the inspectors general have reported on the persistent information security weaknesses that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. 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.¹ Moreover, as we recently testified, VA has faced long-standing challenges in ensuring the security of its systems and information.²

You asked us to examine VA's efforts to address information security vulnerabilities. Our specific objective for this review was to determine the extent to which selected, previously identified vulnerabilities continue to exist on VA computer systems.

To accomplish our objective, we reviewed actions taken to address vulnerabilities that had been identified by VA's Network and Security Operations Center (NSOC). Specifically, we reviewed the details of a critical incident that NSOC had detected in which VA's network had been compromised and the department's efforts to respond to it. This incident was highlighted in a June 2013 testimony by VA's former Chief

¹GAO, *High-Risk Series: An Update*, [GAO-13-283](#) (Washington, D.C.: Feb. 14, 2013).

²GAO, *Information Security: VA Needs to Address Long-Standing Challenges*, [GAO-14-469T](#) (Washington, D.C.: Mar. 25, 2014).

Information Security Officer.³ We also reviewed vulnerabilities NSOC had identified in two key VA web applications⁴ that process veterans' sensitive personally identifiable information. Further, we examined vulnerabilities identified on devices connected to VA's network. To assess the department's efforts in remediating these vulnerabilities, we reviewed tests performed by NSOC, including tests of the two key web applications and network vulnerability test results; interviewed VA officials, including NSOC staff, information security officials, software developers, and VA Office of Inspector General officials; and reviewed VA security policies and guidance, National Institute of Standards and Technology guidance, and prior GAO reports.

We conducted this performance audit from February 2014 to November 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objective. Appendix I provides additional details on our scope and methodology.

Background

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive medical care, benefits, social support, and memorials. VA is one of the largest federal departments, with more than \$150 billion in obligations and a workforce of approximately 313,000 employees for fiscal year 2013. VA is responsible for administering health care and other benefits that directly affect the lives of about 22 million veterans and eligible members of their families.

The department is to provide these services through the Veterans Health Administration, Veterans Benefits Administration, and the National

³ Jerry L. Davis, Former Deputy Assistant Secretary for Information Security, Office of Information and Technology, U.S. Department of Veterans Affairs, testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives, 113th Cong., 1st sess., June 4, 2013.

⁴ 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 via a web browser, such as Internet Explorer.

Cemetery Administration. VA serves over 6 million patients at 151 medical centers, provides compensation and benefits for about 4 million veterans and beneficiaries, and maintains about 3 million gravesites at 131 properties.

In carrying out its mission, VA collects and maintains sensitive medical records and personally identifiable information (PII) of veterans through the use of medical, administrative, and financial computer applications. For example, the department stores veterans' admission, diagnosis, surgical procedure, and discharge information for each stay at a VA medical center, nursing home, or domiciliary, as well as storing PII such as Social Security numbers. Each of the medical centers, which are located around the country, uses local computer systems to run these standard applications. In addition, in providing oversight for disability assistance and economic opportunity to veterans, VA maintains information such as compensation, pension, insurance, and benefits assistance services, as well as educational, loan, and vocational rehabilitation and employment services data.

In providing health care and other benefits to veterans and their dependents, VA relies on a vast array of information technology systems and networks, which supports its operations and stores sensitive information, including medical records and PII. Without proper safeguards, these computer systems are vulnerable to significant risks, including loss or theft of resources; inappropriate access to and disclosure, modification, or destruction of sensitive information; use of computer resources for unauthorized purposes or to launch attacks on other computer systems; and embarrassing security incidents that erode the public's confidence in the agency's ability to accomplish its mission.

Cyber-based threats are evolving and growing and arise from a wide array of sources. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems, as well as user error. Intentional threats can come from sources both internal and external to the organization. Internal threats include fraudulent or malevolent acts by employees or contractors. External threats include the ever-growing number of cyber-based attacks that can come from hackers, criminals, foreign nations, and other sources. These threat sources can exploit vulnerabilities such as those resulting from flaws in software code that could cause a program to malfunction.

Reports of incidents affecting VA's systems and information highlight the serious impact that inadequate information security can have on, among other things, the confidentiality, integrity, and availability of veterans' personal information. For example:

- In January 2014, a software defect in VA's eBenefits system—a web application used by over 2.8 million veterans to access information and services—improperly allowed users to view the personal information of other veterans. According to an official from VA's Office of Information and Technology, this defect potentially allowed 5,399 users to view data of 1,301 veterans or their dependents.
- In June 2013, VA's former Chief Information Security Officer testified that in 2010 VA's network had been compromised by uninvited visitors—nation-state-sponsored attackers—and that attacks had continued. He stated that these attackers were taking advantage of weak technical controls within VA, including those for web applications that contained common exploitable vulnerabilities. He further stated that these resulted in unchallenged and unfettered access to and exploitation of VA systems and information by this specific group of attackers.

The Federal Information Security Management Act of 2002 (FISMA) sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.⁵ FISMA requires each agency to, among other things, develop, document, and implement an agency-wide information security program, using a risk-based approach to information security management. Such a program includes planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies.

The act also assigned the National Institute of Standards and Technology (NIST) responsibility for developing standards and guidelines that include minimum information security requirements. For example, NIST specifies requirements for testing vulnerabilities, remediating them, and developing plans of action and milestones for information systems.

⁵FISMA was enacted as title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

Information Security Responsibilities at VA

At VA, the Assistant Secretary for Information and Technology, who serves as the agency's Chief Information Officer (CIO), is responsible for ensuring that information systems operate at an acceptable level of risk. The CIO reports annually to the head of VA on the overall effectiveness of VA's information security program, including the progress of remedial actions. The CIO designated a Chief Information Security Officer (CISO) who, among other things, manages the development and maintenance of information security policies, procedures, and control techniques to address applicable requirements.

The CISO also heads the department's Office of Information Security, which is responsible for the department's system authorization process, including ensuring plans of action and milestones are maintained. Also within the Office of Information Security, NSOC is responsible for performing vulnerability and compliance scans. Among other things, NSOC may detect incidents such as network intrusions, test web applications for security vulnerabilities, and scan VA's network to test devices connected to the network for known vulnerabilities.

In addition, under the direction of the CIO, the Deputy CIO for Service Delivery and Engineering and system owners are responsible for the overall procurement, development, integration, modification, daily operation, maintenance, and disposal of VA information and information systems. These responsibilities include ensuring (1) that the secure baseline configuration for each system is documented and approved by the authorizing official prior to implementation; (2) compliance with federal security requirements and VA security policies; and (3) remediation and updating of plans of action and milestones and completion of other reviews.

Previously Identified Information Security Challenges

As we recently testified, VA has faced long-standing challenges in effectively implementing its information security program.⁶ Specifically, from fiscal year 2007 through 2013, VA has consistently had weaknesses in key information security control areas. In addition, in fiscal year 2013, the department's independent auditor reported, for the 12th year in a row, that weaknesses in information system controls over financial systems constituted a material weakness. Further, the department's inspector

⁶[GAO-14-469T](#).

general has identified development of an effective information security program and system security controls as a major management challenge for VA. These findings are consistent with challenges GAO has identified in VA's implementation of its security program going back to the late 1990s.

Although VA Has Taken Mitigation Actions, Previously Identified Vulnerabilities Continue to Exist

While VA has taken actions to mitigate previously identified security vulnerabilities, they were insufficient to ensure that these weaknesses were fully addressed. Specifically, VA took steps to contain and eradicate an incident involving intrusion of its network, but these activities were not fully effective. In addition, VA took insufficient actions to address vulnerabilities in two key web applications. Finally, weaknesses identified on VA's workstations (e.g., laptop computers) had not been corrected in a timely manner. Collectively, these weaknesses increase the risk that sensitive data—including veterans' personal information—could be compromised.

VA Could Not Demonstrate That Its Response to a Security Incident Was Effective

Upon detection of an incident, NIST requires that agencies document actions taken in analyzing, containing, eradicating, and recovering from the incident. Specifically, agencies should create follow-up reports for each incident and keep them for a period of time as specified in record retention policies. Organizations should establish a policy for how long evidence from an incident should be retained, taking into account factors such as providing evidence for law enforcement, data retention policies, and cost. Moreover, NIST directs agencies to follow National Archives and Records Administration (NARA) guidance, which states that agency records related to computer security incident handling should be maintained for 3 years.⁷ NIST guidance also notes the importance of agencies having tools in place to aid in incident response.

VA took actions to contain and eradicate an incident detected in 2012 involving an attack by malicious outsiders. VA's NSOC had analyzed the scope of the incident and documented actions taken in response. For example, center staff identified hosts that they believed were affected by the event and took actions to eradicate the effects from these hosts. They

⁷National Archives and Records Administration, *General Records Schedule 24: Information Technology Operations and Management Records*, Transmittal No. 22 (April 2010).

documented the actions taken to address the incident to the point where they believed the incident had been successfully remediated.

However, VA could not provide sufficient documentation to demonstrate that these actions were effective. This is consistent with our findings from a recent government-wide review, in which we estimated that agencies were not able to effectively demonstrate actions taken in response to detected incidents in about 65 percent of cases.⁸ For this particular incident at VA, staff could not locate the associated forensic analysis report or other key materials. Officials explained that digital evidence was only maintained for 30 days due to storage space constraints. As a result, we could not determine the effectiveness of actions taken to address this incident.

Subsequent to this incident, VA established a standard operating procedure that requires the forensic analysis report and related documentation to be maintained for 6 years but allows digital evidence collected during a forensic analysis to be purged 1 month after the completion of the associated forensic analysis report. However, purging such evidence after 1 month is not consistent with NIST-recommended NARA guidance, which calls for records related to computer security incident handling to be maintained for at least 3 years. Without maintaining evidence of incidents, VA cannot demonstrate the effectiveness of its incident response activities and will be unable to use these records to assist in handling future incidents or aiding law enforcement authorities in investigating and prosecuting crimes.

In addition, VA has not yet addressed an underlying vulnerability that contributed to the intrusion. Specifically, VA had planned to implement a solution that would have corrected the weakness in February 2014, but at the time of our review, the solution had not been implemented. VA did take other actions to mitigate the weakness—specifically, limiting the use

⁸GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, [GAO-14-354](#) (Washington, D.C.: Apr. 30, 2014). For that review, we randomly selected 40 incidents from each of 6 randomly selected agencies. This statistical sample allowed us to project the results, with 95 percent confidence, to the 24 major agencies covered by the Chief Financial Officers Act. Based on our sample, we are 95 percent confident that the estimate falls between 58 percent and 72 percent. This estimate represents the percentage of incident cases where the agency did not complete and/or document incident response activities completed for each of the phases—analysis, containment, eradication, and recovery—where required to do so.

of the affected system. However, this is insufficient to prevent recurrence of a similar incident. Until this weakness is fully addressed, or additional mitigating controls are applied, unnecessary risk exists that an incident of this type could recur.

More broadly, NSOC did not have sufficient visibility into VA's computer networks. NIST Special Publication 800-61 states that incident response policies should identify the roles, responsibilities, and levels of authority for those implementing incident response activities.⁹ However, VA's policies did not define the authority for NSOC's access to logs of activity on VA's network that are collected at VA's data centers. As a result, the NSOC cannot be assured that the incident was effectively contained and eradicated from VA's network. As we reported in April 2014, VA's incident response policies defined roles and responsibilities but did not include authorities for the incident response team.¹⁰ Accordingly, we recommended, among other things, that VA revise its policies for incident response by including requirements for defining the incident response team's level of authority. VA concurred with this recommendation. Implementing this recommendation should include providing the NSOC with appropriate authority to review logs of activity on VA's network.

NSOC has initiatives under way to further improve incident response capabilities. For example, it is performing an analysis to determine how best to further restrict access to the VA network and is planning to purchase new incident response tools. However, it has not established a time frame for completing these actions. As noted in our prior work, elements such as specific actions, priorities, and milestones are desirable for evaluating progress, achieving results within specific time frames, and ensuring effective oversight and accountability.¹¹ Until VA's NSOC

⁹NIST, *Computer Security Incident Handling Guide*, Special Publication 800-61, revision 2 (Gaithersburg, Md.: August 2012). NIST states that the policy should also include levels of authority; the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity; the requirements for reporting certain types of incidents; the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels); and the handoff and escalation points in the incident management process.

¹⁰[GAO-14-354](#).

¹¹These elements are discussed in, among other places, GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

establishes such elements, it remains to be seen whether the initiatives will improve its incident response capabilities.

Without assurance that incidents have been effectively contained and eradicated, or the underlying weaknesses effectively mitigated, VA is at increased risk that veterans' PII and other sensitive data may be illicitly modified, disclosed, or lost.

VA Did Not Address All Weaknesses Identified in Key Web Applications

NIST guidance and VA policy both require applications to be tested prior to authorization in order to detect security weaknesses or vulnerabilities. NIST also recommends that organizations develop plans of action and milestones to address these weaknesses. Such plans provide a prioritized approach to risk mitigation and can be used by officials to monitor progress in correcting identified weaknesses.

NSOC tests VA's web applications as part of VA's system authorization process and also conducts tests to validate that corrective actions have been taken to remediate identified vulnerabilities. For two high-impact web applications we reviewed, NSOC had identified four vulnerabilities that it considered high risk for each of the applications. For one of the applications, it also identified a critical vulnerability affecting the protection of PII.

As of June 2014, VA had corrected six of the nine identified vulnerabilities, including the critical PII vulnerability, which it had corrected within 1 week of discovery. However, correction of one of the vulnerabilities had not yet been validated by NSOC for one of the web applications—and had been outstanding for over a year—and two had not yet been validated for the other application. Table 1 shows the status of the nine identified critical and high-risk vulnerabilities.

Table 1: Status of Critical and High-Risk Vulnerabilities Identified in Two Key VA Web Applications

Application	Vulnerability	Date identified by Network and Security Operations Center (NSOC)	Date NSOC validated corrective action	Time from identification of vulnerability to validation of corrective action
1	1	3/26/13	10/3/13	191 days
	2	3/26/13	7/8/13	104 days
	3	3/12/13	Not validated	N/A
	4	3/12/13	4/10/14	394 days
2	1	7/10/12	1/18/14	557 days
	2	7/10/12	1/18/14	557 days
	3	1/22/14	Not validated	N/A
	4 ^a	1/22/14	1/28/14	6 days
	5	1/22/14	Not validated	N/A

Source: GAO analysis of VA data. | GAO-15-117

^aThis vulnerability was the critical PII-related vulnerability.

VA did not provide evidence that it had developed plans of action and milestones for the identified vulnerabilities for which mitigation activities had not been completed. Without plans of action and milestones for correcting high-risk vulnerabilities, VA has less assurance that these weaknesses will be corrected in a timely and effective manner. This, in turn, could lead to unnecessary exposure of veterans' sensitive data that are maintained by these applications.

Various tools, such as "static analysis" tools, can scan software source code, identify root causes of software security vulnerabilities, and correlate and prioritize results. NIST 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.

However, VA did not conduct such analyses for both of the web applications we reviewed. According to VA officials from the Office of Cybersecurity, the department began conducting source code reviews using a static analysis tool in January 2013. Although developers for both of the applications had received the scanning tool, only developers for one of the applications had begun performing source code scans at the time of our review. According to VA officials, they have drafted a policy requiring the use of static analysis tools and it is in the executive approval process. Until VA ensures that its key web applications undergo source code scanning, it risks not detecting critical security vulnerabilities.

Vulnerabilities Identified in Workstations Continued to Exist

NIST guidance and VA policy both require periodic vulnerability scanning,¹² including scanning for patch levels; assessment of risk and risk-based decisions; and tracking and verifying remedial actions, such as applying patches to identified vulnerabilities. In addition, a 2012 VA memo requires that critical patches be applied within 30 days. VA reiterated this requirement in a February 2014 memorandum on patch management and elaborated on its policy. Specifically, the 2014 memorandum states, among other things, that in cases where patches cannot be applied or impact availability, features, or functionality, the department will work with system personnel to develop short-term compensating controls and longer-term plans to migrate to newer platforms, hardware, and/or technologies where security patches can be applied and new security features enabled.

VA periodically scans its network devices—predominantly workstations (e.g., laptop computers)—to identify vulnerabilities that have been identified by software vendors. The department's NSOC scans workstations across VA's network at least monthly and develops executive summaries that show, among other things, the most critical vulnerabilities, such as those requiring patches to remediate them.

However, VA has not always addressed these vulnerabilities in a timely fashion consistent with department policy. As of May 2014, the 10 most prevalent critical vulnerabilities identified by VA's 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 of the 10 missing patches, ranging from approximately 9,200 to 286,700; and
- each patch is intended to mitigate multiple potential known vulnerabilities, ranging from 5 to 51 vulnerabilities, with an average of about 30 and a total of 301 vulnerabilities.

One reason that some of these vulnerabilities continued to exist is that VA decided not to apply patches for the top three vulnerabilities until further

¹²Vulnerability scanners are software tools that, according to NIST, are commonly used in organizations to identify known vulnerabilities on networks and on commonly used operating systems and applications. These scanning tools can proactively identify vulnerabilities, provide a fast and easy way to measure exposure, identify out-of-date software versions, validate compliance with an organizational security policy, and generate alerts and reports about identified vulnerabilities.

testing could determine the effect the patches would have on various applications. However, this decision was not timely. The decision memorandum was dated April 2014, even though the patches covered by the decision had been available from 3 to 10 months, exceeding the 30-day period for critical patches. In this decision memo, the department did not describe whether it had developed compensating controls to address instances where patches were not applied or discuss longer-term plans to migrate to newer platforms, hardware, and/or technologies where security patches can be applied and new security features enabled, as called for by its 2014 patch management memorandum. For the other patches, VA did not provide any documentation of decisions not to apply them. At the end of our audit, VA officials told us they had implemented compensating controls, but did not provide sufficient detail for us to evaluate their effectiveness. Without applying patches or developing compensating controls, VA increases the risk that known vulnerabilities could be exploited, potentially exposing veterans' information to unauthorized modification, disclosure, or loss.

Our findings are consistent with those of VA's Office of Inspector General (OIG), which identified patch management as an issue in its fiscal year 2013 FISMA report.¹³ Specifically, the report identified significant deficiencies in configuration management controls intended to ensure that VA's critical systems have appropriate security baselines and up-to-date vulnerability patches. The OIG found that VA had unsecure web application servers, excessive permissions on database platforms, a significant number of outdated and vulnerable third-party applications and operating system software, and a lack of common platform security standards across the department. To address these issues, the OIG recommended that VA implement a patch and vulnerability management program. In its response to the report, VA stated that in February 2013 it had implemented vulnerability scanning and continued to build on and improve its patch and vulnerability program and that the OIG's recommendation should therefore be closed. However, as our findings suggest, the department has not yet effectively implemented a program to manage vulnerabilities and apply associated patches. Until it does so, it will remain at increased risk that known vulnerabilities could be exploited.

¹³VA Office of Inspector General, *Department of Veterans Affairs: Federal Information Security Management Act Audit for Fiscal Year 2013*, 13-01391-72 (Washington, D.C.: May 2014).

In addition, the scanning procedures that VA used may not detect certain vulnerabilities. Specifically, for Windows systems, VA scanned in “authenticated” mode, but for other systems, such as Linux, its scans were performed in “unauthenticated mode.”¹⁴ The vendor of the scanning tool used by VA recommends scanning in authenticated mode. The unauthenticated scans cannot check for certain patches, potentially allowing for multiple vulnerabilities on these systems to go undetected. This increases the risk that VA would not detect vulnerabilities and take steps to mitigate them, which could allow users to escalate privileges, crash the system, gain administrator access, or manipulate network traffic.

VA also has an initiative under way to facilitate the remediation of known vulnerabilities. In May 2013, it established an organization tasked with overseeing the Service Delivery and Engineering group’s process for

- identifying, prioritizing, and remediating vulnerabilities on VA information systems;
- ensuring baseline configurations and security standards are updated as new vulnerabilities are discovered and remediated;
- ensuring software standards are continually reviewed and updated and that installed software versions comply with these standards;
- identifying, collecting, analyzing, and reporting performance metrics to measure the effectiveness of the patch and vulnerability management, baseline configuration maintenance, and software standards maintenance processes; and
- proposing changes to improve these processes.

This organization has taken initial steps to carry out its responsibilities. For example, it plans to create a database to track remediation and patch implementation. However, VA has yet to identify specific actions, priorities, and milestones for accomplishing these tasks. As noted previously, elements such as specific actions, priorities, and milestones are desirable for evaluating progress, achieving results in specific time frames, and ensuring effective oversight and accountability. Until VA establishes these elements for the new organization, it does not have assurance that these efforts will be effective.

¹⁴Unauthenticated scanning tests a system without using credentials, such as a user ID-password combination. Authenticated scanning, by contrast, tests as a logged-in user and results in the examination of additional security controls.

Conclusions

Ensuring effective security over its information and systems continues to be a challenge for VA. While the department has taken steps to respond to incidents and identify and mitigate vulnerabilities, more can be done to fully address these issues. Specifically, by not keeping sufficient records of its incident response activities, VA lacks assurance that incidents have been effectively addressed and may be less able to effectively respond to future incidents. In addition, without fully addressing an underlying vulnerability that allowed a serious intrusion to occur, increased risk exists that such an incident could recur. While VA has efforts under way to improve its incident response capabilities, until it identifies specific actions, priorities, and milestones for completing these efforts, it will be difficult to gauge its progress. Further, limitations in VA's approach to identifying and addressing vulnerabilities in key web applications, such as not developing plans of action and milestones to address identified vulnerabilities and not scanning all application source code for defects, put veterans' sensitive information at greater risk of compromise. Moreover, VA has yet to fully implement an effective program for identifying and mitigating vulnerabilities in workstations and other network devices, including applying security patches, performing an appropriate level of scanning, and identifying compensating controls and mitigation plans. These shortcomings leave its networks and devices susceptible to exploitation of known security vulnerabilities. While the department has established an organization intended to improve remediation efforts, without identifying specific actions, priorities, and milestones for accomplishing these tasks, this organization's effectiveness will be limited.

Recommendations for Executive Action

To address previously identified security vulnerabilities, we are recommending that the Secretary of Veterans Affairs take the following eight actions:

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

-
- Apply missing critical security patches within established time frames, or in cases where security patches cannot be applied, document compensating controls or, as appropriate, longer-term plans to migrate to newer platforms, hardware, and/or technologies where security patches can be applied and new security features enabled.
 - Scan non-Windows network devices in authenticated mode.
 - Identify specific actions, priorities, and milestones for accomplishing tasks to facilitate vulnerability remediation.

Agency Comments and Our Evaluation

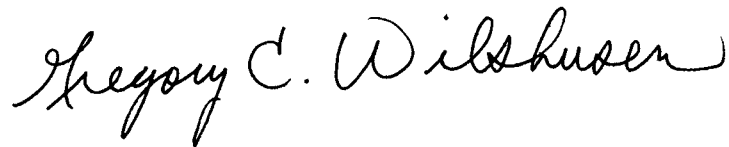
We provided a draft of this report to VA for review and comment. In its written comments (reprinted in appendix II), VA stated that it generally agreed with our conclusions and concurred with our recommendations. VA also stated that it has already taken actions to address six of our eight recommendations and has plans in place to address the remaining two.

Although we have not yet validated the actions described or determined whether they effectively address the issues raised in this report, we are concerned that the actions VA described as completed for at least two of the six recommendations may not comprehensively address the weaknesses we identified. Specifically, for our recommendations related to applying critical security patches and establishing milestones and priorities for facilitating vulnerability remediation, VA's comments focus on its monthly scans, among other things, but do not address application of patches, or identification of milestones and priorities. In this report, we recognize the importance of the monthly scans conducted by the department in accordance with NIST guidance and VA policy. While we acknowledge that VA has efforts underway to address previously identified weaknesses, until it comprehensively and effectively addresses the weaknesses, sensitive personal information entrusted to the department will be at increased risk of unauthorized access, modification, disclosure, or loss. We believe that our recommendations, if effectively implemented, should help the department improve its security posture. We intend to monitor VA's implementation of our recommendations.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 4 days from the report's date. At that time, we will send copies of this report to the appropriate congressional committees, the Secretary of Veterans Affairs, and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, 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. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues



Dr. Nabajyoti Barkakati
Director, Center for Science, Technology, and Engineering

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which selected, previously identified vulnerabilities continue to exist on Department of Veterans Affairs (VA) computer systems.

To address this objective, we reviewed actions taken to address vulnerabilities that had been identified by VA's Network and Security Operations Center (NSOC). Specifically, we reviewed the details of a critical incident that NSOC had detected in which VA's network had been compromised and the department's efforts to respond to it. We selected this incident because it was highlighted in a June 2013 testimony by VA's former Chief Information Security Officer.¹ We reviewed a detailed investigation report prepared by NSOC and interviewed center officials regarding actions taken to detect, analyze, contain, eradicate, and recover from this incident. We also reviewed an internal memorandum related to an underlying vulnerability that contributed to this incident. We compared VA's efforts to address this incident to National Institute of Standards and Technology (NIST) guidance on security controls and incident handling.² We also reviewed VA's standard operating procedure for forensics analysis and compared it to guidance issued by the National Archives and Records Administration.³ We also reviewed a prior GAO report on agencies' (including VA's) incident response practices.⁴ Further, we interviewed NSOC officials to determine what initiatives the department has planned or under way to further improve incident response capabilities.

We also reviewed vulnerabilities NSOC had identified in two key VA web applications. We selected these applications based on their processing of

¹Jerry L. Davis, Former Deputy Assistant Secretary for Information Security, Office of Information and Technology, U.S. Department of Veterans Affairs, testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives 113th Cong., 1st sess., June 4, 2013.

²NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013); *Computer Security Incident Handling Guide*, Special Publication 800-61, revision 2 (Gaithersburg, Md.: August 2012).

³National Archives and Records Administration, *General Records Schedule 24: Information Technology Operations and Management Records*, Transmittal No. 22 (April 2010).

⁴GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, [GAO-14-354](#) (Washington, D.C.: Apr. 30, 2014).

veterans' sensitive personally identifiable information. For these web applications, we reviewed the results of NSOC testing, particularly findings that the testers had categorized as critical or high risk, and compared the dates the vulnerabilities were identified and the dates corrective actions were validated. We also met with VA information security officials and web application developers to determine (1) if plans of actions and milestones had been developed for uncorrected vulnerabilities and (2) the extent to which the department was using tools to conduct software code reviews in order to identify root causes of software vulnerabilities. We evaluated VA actions in accordance with NIST guidance on security testing, developing plans of actions and milestones, and vulnerability analysis⁵ and VA's policy on testing applications prior to authorization.

In addition, we examined vulnerabilities that NSOC had identified on devices connected to VA's network through its monthly vulnerability scans, as well as the settings for the tool NSOC used to conduct these scans. Specifically, we reviewed the results of its May 2014 network scan and further evaluated the 10 most prevalent critical vulnerabilities identified. For these 10 vulnerabilities, which involved missing software patches, we determined the availability of vendor patches, the number of occurrences across VA, and the number of potential known vulnerabilities covered by these patches. We also reviewed an internal memorandum related to delays in installing some of these patches. To determine if VA had initiatives under way to facilitate remediation of these vulnerabilities, we met with officials from VA's Service Delivery and Engineering organization. We also reviewed NIST guidance on vulnerability scanning,⁶ internal VA memorandums from 2012 and 2014 outlining patch management requirements, VA's Office of Inspector General 2013 report on the department's compliance with the Federal Information Security Management Act,⁷ and vendor documentation related to a vulnerability scanning tool used by VA.

⁵NIST, Special Publication 800-53, rev. 4.

⁶NIST, Special Publication 800-53, rev. 4.

⁷VA Office of Inspector General, *Department of Veterans Affairs: Federal Information Security Management Act Audit for Fiscal Year 2013*, 13-01391-72 (Washington, D.C.: May 2014).

We conducted this performance audit from February 2014 to November 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objective.

Appendix II: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

October 31, 2014

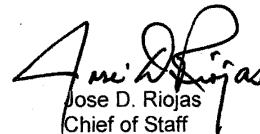
Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, "**INFORMATION SECURITY: VA Needs to Address Identified Vulnerabilities**" (GAO-15-117). VA generally agrees with GAO's conclusions and concurs with GAO's recommendations to the Department.

The enclosure specifically addresses GAO's recommendations and provides an action plan for each. VA appreciates the opportunity to comment on your draft report.

Sincerely,


Jose D. Riojas
Chief of Staff

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: VA Needs to Address Identified Vulnerabilities"
(GAO-15-117)

GAO Recommendation: To address previously identified security vulnerabilities, GAO is recommending that the Secretary of Veterans Affairs take the following eight actions:

Recommendation 1: Update the department's standard operating procedure to require evidence associated with security incidents to be maintained for at least 3 years, consistent with NARA guidance.

VA Comment: Concur. The Department of Veterans Affairs (VA) has validated and modified its internal standard operating procedures to ensure it maintains records regarding major cyber incidents requiring detailed investigations for 3 years, per National Archives and Records Administration guidance. On an average week, VA blocks approximately 13 million email messages by a reputation filter, and approximately 32 million malware instances are stopped by VA's defense in-depth security strategy. These attempts to harm VA's enterprise can exceed 905 million messages and 1.7 billion malware instances per year. The recommendation to maintain records on these activities would exceed the resources available for VA to effectively manage and maintain the evidence. As a result, VA will only maintain major incidents. VA requests closure of this recommendation.

Recommendation 2: Fully implement the solution to address the weaknesses that led to the 2012 intrusion incident.

VA Comment: Concur. VA's internal Deep Dive Analysis Team developed a list of recommended actions that would mitigate VA's exposure highlighted by the 2012 incident. As a result of these recommendations, VA has implemented multiple information security practices and solutions to address those recommendations. As a result, VA has put into place the following actions and activities as part of its standard security procedures:

- Enhanced monitoring of all Active Directory Servers.
- Mandating that Accounts with Domain Administrative privileges cannot be the same as a user's Domain login account.
- Mandating multifactor authentication for accounts with Domain Administrative privileges.
- Capability to calculate the distance/time between logins and identify logins to indicate compromised login credentials.
- Functionality to automatically ingest Indicators of Compromise (IOC) from US-CERT and other sources, and then automatically correlate them against multiple log sources over regular intervals.
- Limiting remote access to VA resources.

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: VA Needs to Address Identified Vulnerabilities"
(GAO-15-117)

- Limiting access to resources and information from outside the continental United States.
- Custom security policies within gateway firewalls for Active Directory servers.
- Aggressive examination and blocking of HTTP communications.
- Configuration of advanced file logging functionality on the gateway firewalls.
- Discontinued use of One-VA Virtual Private Network.
- Blocking all requests for dynamic Domain Name System Domains.

In response to this incident, VA procured a full packet capture system for the gateways to provide a historical record of all network traffic traversing the gateways. VA also developed custom McAfee Host Intrusion Prevention Security (HIPS) signatures to detect IOCs specific to Advanced Persistent Threat groups and deployed an automated dynamic unknown file analysis and protection solution in all four Trusted Internet Connection gateways and in five major VA data centers. VA is also piloting a proactive exploit prevention agent to provide enhanced protection from successful exploitation of systems. In addition, VA created a dedicated Cyber Threat Intelligence Team to focus on the collection of threat intelligence from various sources and collaboration with other government organizations such as US-CERT and the Department of Health and Human Services. VA also procured compromise assessment services to perform independent assessments of VA's critical network infrastructure. VA continues to enhance its cyber security posture in light of emerging threats. In light of the above cyber security activities and improvements, VA believes it has fully mitigated the risks associated with the 2012 incident, and VA requests closure of this recommendation.

Recommendation 3: Establish time frames for completing planned initiatives to improve incident response capabilities.

VA Comment: Concur. VA maintains a robust incident response capability that allows for rapid assessment and appropriate action(s) across the enterprise. As noted in VA's response to recommendations outlined in *"INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices"* (GAO 14-354), VA has implemented or will complete enhancements to its incident response mechanisms by March 2015. VA has implemented a phased training program that targets staff responsible for cyber incident response. VA has worked closely with the Department of Homeland Security (DHS) to test VA's incident response capability on numerous occasions in 2014, and DHS is scheduled to retest VA's incident response capability in the spring of 2015. In addition, VA exercises its incident response capabilities every day in responding to the daily threats that are detected throughout its networks and systems.

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: VA Needs to Address Identified Vulnerabilities"
(GAO-15-117)

GAO Recommendation 4: Develop plans of action and milestones for critical and high-risk vulnerabilities affecting two key web applications.

VA Comments: Concur. VA application project managers for both key Web applications have outlined remediation steps for all remaining application risks, with plans to remediate the outstanding risks during their November 2014 release dates. VA requests closure of this recommendation.

Recommendation 5: Finalize and implement the policy requiring developers to conduct source code scans on key web applications.

VA Comment: Concur. VA Handbook 6500 requires the implementation of *Security Control RA-5 Vulnerability Scanning*, which establishes a requirement for the scanning of information systems and as required, a source code review and source code analysis for key VA applications. In addition, *Security Control SA-4 Acquisition Process* requires the design and implementation of security controls that may include source code reviews. Furthermore, VA has also procured and implemented a source code security analysis tool that it uses to perform security analysis and reviews on a number of key VA applications. VA will issue a policy memorandum in the first quarter of fiscal year (FY) 2015 to specifically require developers to conduct source code scans for the most critical VA applications, to include key Web applications. Moreover, VA regularly conducts Web application security assessments on externally and internally-facing applications as part of its defense in-depth security strategy. VA requests closure of this recommendation.

Recommendation 6: Apply missing critical security patches within established time frames, or in cases where security patches cannot be applied, document compensating controls or, as appropriate, longer-term plans to migrate to newer platforms, hardware, and/or technologies where security patches can be applied and new security features enabled.

VA Comment: Concur. VA operates a national patch management program which focuses on assessing the risk to the enterprise in relation to the impact on Veteran safety and the operational needs of the Department. VA is continually working to improve the effectiveness of its vulnerability management program as part of VA's Continuous Readiness in Information Security Program (CRISP). As a result of the continuous improvement methodology, VA has developed a plan that calls for improving metrics, identifying gaps in tools and/or processes, implementing vulnerability management databases for tracking, and executing scans for the differing technologies within the enterprise, to include remediation and validation. VA has also developed an aggressive vulnerability assessment plan that includes detailed monthly enterprise scanning across the enterprise. VA requests closure of this recommendation.

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: VA Needs to Address Identified Vulnerabilities"
(GAO-15-117)

Recommendation 7: Scan non-Windows network devices in authenticated mode.

VA Comment: Concur. While a majority of VA's networks are Windows-based, VA is evaluating how to implement credentialed scanning of the approximately 10 percent of systems that are scanned un-credentialed. VA expects to complete this evaluation and implement credentialed scanning of non-Windows devices by third quarter, FY 2015.

Recommendation 8: Identify specific actions, priorities, and milestones for accomplishing tasks to facilitate vulnerability remediation.

VA Comment: Concur. VA has an effective vulnerability management program to support CRISP. As part of its defense in-depth security strategy, VA has developed an aggressive vulnerability assessment plan that includes monthly enterprise scanning to enumerate patch and configuration flaws across the enterprise. VA requests closure of this recommendation.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov
Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Jeffrey Knott, Lon Chin, Harold Lewis, and Chris Warweg (assistant directors); Jennifer R. Franks; Lee McCracken; and Tyler Mountjoy made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

