Department of Veterans Affairs
Office of Inspector General

Administrative Investigation
Improper Access to the VA Network by VA Contractors from Foreign Countries
Office of Information and Technology
Austin, TX

Redacted

Report No. 13-01730-159

April 13, 2015

VA Office of Inspector General
Washington, DC 20420

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington, DC 20420

TO: VA Chief of Staff

SUBJECT: Administrative Investigation, Improper Access to the VA Network by VA Contractors from Foreign Countries, Office of Information and Technology (OIT), Austin, TX (2013-01730-IQ-0160)

Summary

In a July 11, 2006, VA Office of Inspector General (OIG) report titled: *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, OIG found that the loss of VA data was possible because a VA employee used "extremely poor judgment" and that VA senior officials failed to take appropriate action to determine the "magnitude and significance" of the incident. They also found that VA information security employees with responsibility for receiving, assessing, investigating, or notifying higher level officials…reacted with indifference, little sense of urgency, or responsibility.

On July 20, 2006, VA's Secretary, R. James Nicholson, provided a written statement to the Senate Veterans' Affairs Committee (SVAC). In his statement, Secretary Nicholson said, "We can make VA the 'Gold Standard' in the area of information security…VA must be the best in the Federal government in protecting personal and health information, training, and educating our employees to achieve that goal. The culture must put the custody of veterans' personal information first, over and above expediency."

In the December 2007 VA Information & Technology Strategic Plan for FY 2006–2011 report, VA's Chief Information Officer (CIO) said that OIT would be centralized under the authority of the CIO, and the CIO identified priorities to address. These included strengthen data security controls within VA and VA contractors to substantially reduce the risk of unauthorized exposure, create an environment of vigilance and awareness to the risks…by integrating security awareness into daily activities, and remedy VA's longstanding IT material weaknesses related to a general lack of security controls.

We found that 7 years after the 2006 data breach, VA information security employees still reacted with indifference, little sense of urgency, or responsibility concerning a possible cyber threat incident. Austin Information Technology Center (AITC) OIT employees failed to follow VA information security policy and contract security

requirements when they approved VA contractor employees to work remotely and access VA's network from China and India. One accessed it from China using personally-owned equipment (POE) that he took to and left in China, and the other accessed it from India using POE that he took with him to India and then brought back to the United States (US). After the Acting CIO learned of this improper remote access, he gave verbal instructions for it to cease; however, VA information security employees at all levels failed to quickly respond to stop the practice and to determine if there was a compromise to any VA data as a result of VA's network being accessed internationally. Further, we found that [redacted] Linux/UNIX Operating Systems, AITC, as a VA employee, as well as other VA contractor employees, improperly connected to VA's network from foreign locations. (b)(6)

Introduction

The VA Office of Inspector General (OIG) Administrative Investigations Division investigated an allegation that OIT employees permitted a VA contractor employee to connect to VA's network from China. Initially, OIG Hotline referred the allegation to Mr. John Killian, Director of VA's Network Security Operations Center (NSOC); however, based on his insufficient response, OIG Hotline referred it to the OIG Administrative Investigations Division. We also investigated whether VA OIT employees responded timely and prudently after learning that VA contractor employees accessed VA's network from foreign countries. To assess these allegations, we interviewed Mr. Killian; [redacted] Enterprise Operations Systems Security; [redacted] VA Enterprise Network Defense for NSOC; Mr. Gary Stevens, Director VA Cyber Security; Mr. Stephen Warren, Executive in Charge and former Chief Information Officer (CIO) for OIT; [redacted] AITC [redacted]; other VA employees; and VA contractor employees. We also reviewed VA network activity, email, personnel, and task order records, as well as applicable Federal laws, regulations, and VA policy. (b)(6)

Background

How Secure is Veterans' Privacy Information?

At a June 4, 2013, hearing before the US House of Representatives, Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, VA's former Deputy Assistant Secretary for Information Security, Mr. Jerry L. Davis, provided the Committee a prepared statement. In it, he said that he began his VA employment in August 2010, and at that time, Mr. Warren told him that there were "uninvited visitors in the network." Mr. Davis said that he learned that these "attackers were a nation-state sponsored cyber espionage unit and that no less than eight (8) different nation-state sponsored organizations had successfully compromised VA networks and data" or they were actively attacking them, taking advantage of "weak technical controls within the VA

network." He further said that he made sure each instance of attack or compromise to VA networks by these attackers was documented and given to VA OIT leadership, to include Mr. Warren. The Chairman of the House Veterans' Affairs Oversight and Investigations Subcommittee said that "evidence suggests" that VA's networks have "repeatedly been compromised since 2010 by foreign actors, including China." Mr. Davis told the Committee that in a February 2013 report published by Mandiant—an American cybersecurity firm that directly implicated China in cyber espionage—they identified "attackers coming from the People's Republic of China, the People's Liberation Army [Chinese military], and…"the Comment Crew [Chinese hackers]… known to be sponsored by the People's Liberation Army." Mr. Warren told the Committee, "We take any potential incident and any incident very seriously. I take it personally… I'm personally responsible for the organization as the Acting CIO." http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg82237/html/CHRG-113hhrg82237.htm

Transformation Twenty-One Total Technology

A February 17, 2011, VA Office of Public and Intergovernmental Affairs news release stated that the purpose of Transformation Twenty-One Total Technology (T4) was to transform VA's IT programs to improve quality of healthcare and benefits services to veterans, their families, and survivors. T4 is a 5-year program to meet the full range of VA's long-term technology needs. The program serves as a single focal point for managing the multiple award contract vehicle giving VA access to the best of industry's capabilities without extended acquisition lead time. It further reflected that the T4 program would consist of up to 15 prime contracts, including four reserved for service-disabled veteran-owned small businesses (SDVOSB) and three reserved for veteran-owned small businesses (VOSB).

Systems Made Simple, Inc. (SMS)

SMS's website reflected that it was founded in 1991 in New York and that they received certification as an SDVOSB in 2004. SMS was selected as one of seven SDVOSBs to support the T4 acquisition project in 2011. Task order records reflected that SMS provided operating system administration for three shifts, 24x7, on identified Unix variants; provided system administration activities and immediate troubleshooting efforts when contacted by the service desk to ensure outages or incidents were resolved for over 1,100 UNIX servers; and worked with customers and partners, end users, programmers and analysts, database administrators, and application and network administrators.

Contract #VA118-11-D-1000

Task order records reflected and [redacted] with VA Technology Acquisition Center (TAC), Eatontown, NJ, confirmed that VA's TAC awarded SMS an Indefinite Delivery/Indefinite Quantity/Multiple Award Task Order in (b)(6)

June 2011. Task order records disclosed and [redacted] confirmed that the period of performance for the basic task order was 5 years from the effective date of the award. A Performance Work Statement (PWS), dated March 2011, reflected that the contractor provide a total IT services solution encompassing, but not limited to, software and IT products incidental to the solution, in conjunction with all services needed to integrate system, network, or other IT service in order to meet a client's mission requirements. (b)(6)

Task order records and a press release reflected that in February 2012 the TAC awarded SMS a performance-based task order, #VA118-1000-0004, "Data Center Acquisitions Transformation Twenty-One Total Technology (DCAT4)," issued on a firm fixed-price and time and materials basis, in accordance with contract #VA118-11-D-1000. The total value of this task order stood at $715 million. Task order records reflected that the following subcontractors/vendors were proposed and accepted for use under this task order: TEKsystems, [redacted] The period of performance included an 8-month base period terminating at the end of fiscal year 2012 followed by four 12-month option periods. This effort was to support the mission of the Corporate Data Center Operations. (b)(4)

Corporate Data Center Operations (CDCO)

Contract records reflected that the mission of VA OIT CDCO stood to provide *One-VA* world-class service to veterans by delivering results-oriented, secure, highly available and cost-effective IT services. Records reflected that CDCO remained a full-service IT provider, offering a wide variety of products and services to its VA and other Federal agency customers. As the corporate IT center for VA's nationwide systems, CDCO supported mission-critical functions through about 200 complex applications and over 2,000 physical and virtual servers. As a Corporate Data Center for VA, AITC provided IT services to VA customers and is a recognized, award-winning Federal data center within VA. In addition to supporting the IT requirements of VA, AITC provides service to a number of other Government agencies. AITC runs more than 100 customer applications and provided mission-critical data for financial management, payroll, human resources, logistics, medical records, eligibility benefits, and supply functions.

Remote Enterprise Security Compliance Update Environment (RESCUE) Government Furnished Equipment (GFE)

Contract records reflected that the objective of RESCUE GFE was to ensure remote access needs were met and VA data and security were not compromised. The user was able to log onto devices for which they had privileges, download VA information to the remote compliant device, print to a local printer, and when connectivity was terminated, any VA data downloaded to the compliant device remained. VA's RESCUE GFE user's guide reflected that RESCUE enhanced remote access capabilities by extending the

network to remote users. The built-in remediation system established that an acceptable level of security existed prior to permitting access to VA protected information. RESCUE was designed and recommended to be the sole solution for GFE devices, and it provided a security posture check, ensuring VA data remained encrypted from the end device into the VA trusted network. Mr. Warren told us that RESCUE on a GFE device, once connected to the network, performed checks on the device to ensure that the proper anti-virus and security patches existed. He said that it was active monitoring of the device and forensic tools deployed on the GFE allowed OIT to "drop endpoint security" on it. He said that the "policy and practice" was to use GFE. He also said that if someone used non-GFE, the same "policy and practice" should apply.

Citrix Access Gateway (CAG)

CAG is a web-based interface that permits the use of POE, but it requires a "plug-in" be installed on the device. The CAG user guide stated that before accessing the external CAG, access must be enabled by the ISO. It also stated that CAG was the recommended and the most secure method when using POE and that when using CAG, the device was never actually on VA's trusted network, providing a virtual desktop. However, it also reflected that a user could copy, paste, or print while on CAG, if the user provided a sufficient business justification to their ISO. The OIT CIO FY 2011 Annual Report reflected that CAG enabled the secure use of non-government furnished equipment for contractors requiring safe, limited access to VA's network; however, the US Computer Emergency Readiness Team (US-CERT) website listed many identified vulnerabilities with CAG. VA OIG's ISO confirmed that the US-CERT among other sources "pointed out vulnerability remediations required for [CAG] infrastructures."

VA and Contractor Employees

[redacted] *VA Enterprise Operations Systems Security* (b)(6)

[redacted] told us that he was in his current position for over 3 years. Personnel records reflected that he was responsible for demonstrating the ability to lead change, to develop, and implement an organizational vision and to balance change and continuity, and make logical decisions that are understood and supported. It also reflected that he was to exercise due diligence or care in efforts to plan, develop, coordinate, and implement an effective information security program, demonstrate accountability, continuous improvement, and make timely and effective decisions. He was responsible to ensure that AITC-managed systems and data were maintained, industry best practices were continually reviewed, and the practices that provide enhanced, cost-effective security safeguards for AITC were implemented. Records reflected that [redacted] efficiently maintained customer support and attended and contributed to multiple OIT

level security councils and working groups, including security improvement program, field operations security council, and security architecture.

Mr. John Killian, (GS-15) former Director, VA NSOC

Mr. Killian told us that as the NSOC Director, he was responsible for the organization with oversight and control of VA enterprise security. He said that any time there was an incident, such as a reported virus, unauthorized access, or malware, his organization conducted the appropriate investigation and mitigation. The NSOC website reflected that they were responsible for protecting VA information on a "24x7 basis" – by monitoring, responding to, and reporting cyber threats and vulnerabilities; managing internet gateways; conducting enterprise-network monitoring; and providing value-added network and security management services as requested. It also reflected that the NSOC was responsible for protecting the confidentiality, integrity, and availability of VA information systems and the data traversing its Enterprise network, design and implement technology to detect and defeat malicious cyber activity directed at the VA Internet Gateways. Further, the NSOC was to provide central coordination and incident response functions for all security and privacy events impacting VA and to provide services that included anti-virus protection, intrusion protection, penetration tests, vulnerability scanning and firewall management in successfully defending the Enterprise network against external threats.

Personnel records reflected that Mr. Killian, as the NSOC Director, provided expert technical analysis, input, and knowledge in support of OIT and information security initiatives, projects and tasks assigned. In a self-assessment, Mr. Killian said that he directed reactive measures to combat several malicious attacks within VA and provided the guidance and leadership in eradicating the threats and that he facilitated the designation of the NSOC as the Computer Security Incident Response Team as well as the Computer Emergency Response Team.

Mr. Stanley Lowe, Deputy Assistant Secretary for Information Security and Chief Information Security Officer, told us that as of November 2014, Mr. Killian was no longer the Director of NSOC, as he (Mr. Lowe) and Mr. Killian's immediate supervisor decided they needed someone more engaged in that position. Personnel records did not reflect Mr. Killian's transfer to another position or a change to his title.

[redacted] *VA Enterprise Network Defense for NSOC* (b)(6)

[redacted] told us that he was appointed in [redacted] 2009. He told us that he supervised both contractor and Government employees who maintained the Enterprise Network Defense section of NSOC. He said that his group performed all the vulnerability scanning for the enterprise, penetration and application testing, threat

reporting services to VA, and deep-dive analysis. Personnel records reflected that he leads organizational elements that have a direct impact on the availability and integrity of network and security centric services delivered to the VA enterprise. His responsibilities included ensuring critical functions within the NSOC were manned 24/7/365; critical personnel were available anytime in the event of emergency operations and that changes to any system, architecture or configuration was vetted through a change control process to allow for documentation of the change, concurrence from other functional areas affected. Records reflected that he provided exemplary support in securing VA's Enterprise Network and provided key investigative reports to advise and educate Executive Management of the immediate threat to VA's computing environment.

[redacted], *SMS Sub-Contractor Employee* (b)(6)

[redacted] told us that he was born in China. He said that he earned his bachelor's degree in chemical physics and master's degree in theoretical chemistry from [redacted], and he earned his Ph.D. in computational chemistry at [redacted]. He said that he was a dual citizen of the US and Canada, claiming Canadian citizenship in 2003 or 2004, and he held a Canadian passport. [redacted] He said that he became a naturalized US citizen in either 2009 or 2010 and that he also held a US passport. He further said that he provided financial support, [redacted] to his family in China.

TEKsystems (TEK) employment records reflected that [redacted] began working for TEK as an HP/UX Administrator on [redacted], 2010. Records of the Texas Comptroller's Office reflected that [redacted] registered as the President and Director of [redacted] Austin, TX, on [redacted], 2010. In a March 12, 2012, email, a TEK systems representative told [redacted], "Thank you for your interest in providing services to TEKsystems through our Sub-Vendor program. We have reviewed your profile questionnaire and would like to continue with establishing our services relationship." TEK records reflected that they entered a Secondary Supplier Service Agreement on March [redacted] 2012.

[redacted] told us that on April 1, 2012, SMS became the primary VA contractor, and TEK became a subcontractor under SMS. He said that his company, [redacted], provided support services to VA under DCAT4 and that TEK remained his only customer. Task order records reflected and [redacted] confirmed that as a Unix System Administrator, he performed functions such as fault isolation and/or systems administration for other Unix-based operating systems; installed, configured, tuned and maintained software; administered user accounts and passwords; maintained system accounting files and logs and system error logs; implemented security structures provided by VA's security division to prevent unauthorized access; and, performed knowledge transfer of critical (b)(6)

HP/UX and Linux system administration tasks to AITC system administrators. Manpower reports and training records reflected that [redacted] completed VA cyber security awareness and rules of behavior training and annual VA privacy training in 2012 and 2013 and that he had a minimum background investigation.

Mr. Stanley Lowe, (SES) Deputy Assistant Secretary for Information Security and Chief Information Security Officer

Mr. Lowe told us that he served in his current position since February 2013 and that he previously served as the Deputy Director for the Department of Defense and VA Interagency Program Office. He described his day-to-day responsibilities as overseeing the following VA programs: Information Security, Records, Privacy, and Policy. He acknowledged that he was responsible for VA's Information Security Program policy, VA Directive/Handbook 6500.

[redacted] *Enterprise Management, VA Enterprise Operations*

(b)(6)

[redacted] told us that he began his VA employment in 2001. He said that he supervised about 50 employees and contractor employees who manage the middleware infrastructure of the VA. He further said that outside the application, database, or operating system, his group managed it, as well as the monitoring and messaging at the VA data centers.

[redacted] *Linux/UNIX Operating Systems, VA Enterprise Operations*

[redacted] was appointed in [redacted] 2000 as a computer specialist, promoted into an IT specialist position, and resigned in [redacted] 2006. [redacted] told us that from [redacted] 2006 to [redacted] 2008 she was on [redacted] and personnel records reflected that in [redacted] 2008, VA reinstated her as an IT specialist. In 2010, she was promoted to a [redacted] position, which she currently holds.

[redacted] *SMS Sub-Contractor Employee*

[redacted] told us that he was born in India and first entered the US in [redacted] 2006. He said that he is a citizen of India, working in the US on an H-1B visa—the H-1B program applies to employers seeking to hire nonimmigrant aliens as workers in specialty occupations. The H-1B provisions help US employers who could not otherwise obtain needed business skills and abilities from the US workforce, by authorizing the temporary employment of qualified individuals who are not otherwise authorized to work in the US.

[redacted] told us that since April 2012 he supported the DCAT4 program through his employer ZENINFOTECH, LLC, which assisted SMS through TEK. He said that he worked with the programs that used WebLogic and also worked as a Monitoring Administrator. Task order records reflected that the contractor must conduct WebLogic server and WebLogic portal architecture and administration involving installation, configuration, tuning, and deploying applications on WebLogic server and portal versions and document, diagnose, and correct problems that occur within installed WebLogic applications. Manpower reports and training records reflected that [redacted] completed VA cyber security awareness and rules of behavior training and annual VA privacy training in 2012 and 2013. He also had a [redacted] background screening. (b)(6)

Mr. Gary Stevens, (GS-15) Director, VA Cyber Security

Personnel records reflected and Mr. Stevens confirmed that he was appointed in December 2011. Personnel records reflected that he managed the assigned Cyber Security Service activities, ensured that risks were identified, and actions were taken to mitigate known risks, provided timely briefings to the supervisor on the nature and policy implications of issues and recommendations reflected through analysis, familiarity with appropriate procedures, programs, and policies, sound judgment and sensitivity to issues.

Mr. Stephen Warren, (SES) former CIO for VA Office of Information Technology

Personnel records reflected that Mr. Warren began working for VA on April 29, 2007. He told us that he was the Acting CIO from March 2013 to March 2015. (The former CIO resigned from the position on March 8, 2013.) Personnel records reflected Mr. Warren's title as Principal Deputy Assistant Secretary for OIT. VA's OIT website reflected that under the direction of the CIO, OIT delivered available, adaptable, secure, and cost-effective technology services to VA and acted as a steward for all VA's IT assets and resources. As VA's Acting CIO, Mr. Warren was responsible for oversight of the day-to-day activities to ensure VA employees had the needed information technology tools and services, and Mr. Warren told us that he was responsible for the operation of VA's information technology infrastructure. VA policy states that the CIO is responsible for ensuring that operating systems under OIT's area of responsibility operate at an acceptable level of risk; develop and maintain information security policies, procedures, and control techniques to address all applicable requirements; oversee personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; order and enforce Department-wide compliance with and execution of any information security policy; and establish and provide supervision over an effective incident reporting system. Mr. Warren told us that VA policy and practice "does not replace good judgment." He said that "policies and directives are the boundaries of the road…there is more than just what the directives tell you. You have got to put some judgment into it."

Results

Issue 1: Whether There Was Improper Access to VA's Network and OIT Employees Failed to Discharge the Duties of Their Positions When They Failed to Quickly Respond to the Improper Access

VA policy states that "telework" means to work from an alternative worksite other than the traditional office setting and the primary intent of the program is to support the mission from an alternative work setting. VA Handbook 5011/5, Paragraph 1 and Part II, Chapter 4 (September 22, 2005). The US Office of Personnel Management (OPM) webpage reference material reflected that the Federal telework program and policies cover only Federal employees and that Federal contractors are not governed by OPM and General Services Administration (GSA) telework guidance or by individual agency policies. It states that contractor telework arrangements should be negotiated with the contractor's employer and the appropriate Federal agency official so that policies and procedures are closely aligned, all parties are in agreement, and telework language may be integrated into the contract. Another OPM telework reference webpage states that Federal agencies and staff are responsible for the security of Federal government property, information, and information systems and that if not properly implemented, telework may introduce vulnerabilities into agency systems and networks. *OPM's Guide to Telework in the Federal Government* (April 2011).

[redacted] told us that for SMS contractor employees, the VA program office identified each position eligible for telework or remote capabilities. The contracting officer representative (COR) was not the authorizing official for contractor employees wanting to telework or work remotely; the COR provided SMS the information of which positions were approved for a consideration of teleworking; and the work schedule was then coordinated between the SMS program management team and the requesting VA program office. However, [redacted] told us that the SMS program management team thought that if it was acceptable with VA, it was acceptable with them. [redacted] said that the teleworking contractor employees requested Virtual Private Network (VPN)/RESCUE access as part of their onboarding process. (b)(6)

Improper Telework Agreements with Contractor Employees

Contract records reflected that efforts under task order #VA118-1000-0004 shall be performed on-site at VA CDCO facilities such as the one located in Austin, TX. A VA telework proposal, dated January 8, 2013, listed [redacted]'s duty station as Austin, TX; however, the proposal reflected that [redacted] signed it on January 9 approving [redacted] to work from his residence in [redacted], MI, every other month from January 2013 to indefinite. [redacted] told us that although VA's telework program did not apply to contractor employees, the task order allowed for contractor employees to work remotely. She said that they used VA's telework form as a matter of convenience, as it contained the necessary information to devise schedules for multiple people. She also said that she (b)(6)

signed [redacted]'s proposal in the supervisor's signature block authorizing it as a matter of "habit" and "for no other reason than it was sitting in front of me and I signed it."

[redacted] told us that since [redacted] was not the CO or COR, she did not have the authority to permit [redacted] to telework or work remotely. [redacted] told us that she and [redacted], talked about [redacted]'s Michigan telework proposal beforehand and agreed that it would work. [redacted] told us that [redacted] told him that the schedule in the telework proposal stood as [redacted]'s schedule. He said that he possibly suggested that [redacted] submit a VA telework proposal, but he remained uninvolved in the decision-making process, because [redacted] turned to [redacted] for an approval. [redacted] Information Security [redacted] told us that he did not know under what authority [redacted] signed [redacted]'s telework proposal, especially on an indefinite basis. (b)(6)

[redacted] told us that he was unaware of any telework agreement that was promulgated for [redacted]. He said that the work statement, paragraph 4.6.1, referenced remote access for the performance of duty, but it did not specifically mention telework. He also said that under the task order, security operations authorized remote access. Task order records reflected that paragraph 4.6.1 stated that contractor employees requiring remote access to VA networks should work with the COR to determine the appropriate access method needed for their situation. [redacted] said that the task order did not address telework agreements, as that remained a VA vernacular and did not apply to contractor employees. He said that certain functions under this task order did not lend themselves to telework; however, the infrastructure service that [redacted] supported allowed for teleworking or working remotely. [redacted] told us that in coordination with [redacted] and SMS, [redacted]'s teleworking from Michigan remained compliant with the task order, but the approval of the COR was required for technical concurrence that the work [redacted] performed could be successfully accomplished without onsite support.

On May 2, 2012, [redacted] signed a VA telework proposal authorizing [redacted] to telework from New York from May 7 to June 15, 2012. [redacted] told us that he signed the document to concur and not to approve [redacted]'s request. He said that the issues with the process and documentation for SMS contractor employees teleworking was resolved at a later date, with SMS now using their own internal process and forms to approve contractor employees teleworking. (b)(6)

[redacted] told us that she spoke with the COR and SMS representative in December 2013, and she told them that VA did not execute employee agreements with contractors. She said that she told them that SMS needed to verify that their files were compliant, and she told us that SMS now ensures explicit, written COR remote/telework approval for each position before considering a contractor employee's request for such.

A February 3, 2014, email reflected that [redacted] agreed to allow [redacted] to telework permanently from his home in Michigan, and [redacted] submitted an SMS telework request to work 5 days a week on a permanent basis from his home. (b)(6)

Improper Teleworking from China

VA policy states that contractor employees must comply with VA's security and data privacy directives and handbooks. VA Handbook 6500.6, Appendix D. It also prohibits the installation and use of personally-owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. Id., at Appendix C. Section C of VA's SMS task order reiterates this prohibition of using personally-owned equipment and the requirement for it to be included in the contract if there was a need to use non-VA owned equipment. It further states that all security controls required for GFE must be used in approved other equipment; all remote systems must be equipped with, and use, a VA-approved antivirus software and a firewall that is configured with a VA-approved configuration; and that the software must be kept current, including all critical updates and patches.

VA's SMS task order states that the contractor shall comply with VA security requirements in accordance with VA Handbook 6500.6 "Contract Security" and Addendum A of the document. It further states that contractor-supplied equipment, PCs of all types, etc., for contract services must meet all security requirements that apply to GFE and Government Other Equipment (GOE). Security requirements include: a) VA approved encryption software installed on all laptops or mobile devices before placed into operation; b) Bluetooth equipped devices are prohibited; Bluetooth must be permanently disabled or removed from the device; c) VA-approved anti-virus and firewall software; and, d) Equipment must meet all VA sanitization requirements and procedures before disposal. Moreover, the COR, CO, the project manager, and the information security officer (ISO) must be notified and verify all security requirements were met. Id., at Addendum A, Paragraph A1.0. It also states that contractors whose personnel require remote access to VA networks should work with the COR to determine appropriate access method needed for their situation.

VA policy further states that an employee will notify their VA supervisor, local CIO and ISO prior to any international travel with a mobile device, i.e. laptop, so that appropriate actions can be taken prior to departure and upon return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return. VA Handbook 6500, Appendix D. It states that VA issues specially configured mobile devices to individuals traveling to locations that VA deems to be of significant risk; and applies inspection and preventative measures to mobile devices returning from locations that VA deems to be of significant risk in accordance with VA policies and procedures. Id., at Appendix F.

Moreover, VA policy states that mobile devices; i.e., notebook/laptop computers, are not allowed access to any VA network without first meeting VA and the facility's security policies, procedures, and configuration standards. These include scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, and conduct primary operating system integrity checks. It also states that to travel outside the US for VA business, OIT must provide the necessary mobile devices that: 1) have been sanitized to remove existing VA information; 2) have limited applications installed; 3) have the most stringent configuration settings possible that still allow the user to perform their required duties; and, 4) are encrypted with FIPS 140-2 (or its successor) validated encryption. VA Handbook 6500, Appendix F.

A VA telework proposal dated January 18, 2013, reflected that [redacted] requested to telework from China from January 29 to February 17, 2013. In a January 23, 2013, email, Subject: Telework Outside of U.S.A., [redacted] told [redacted] AITC [redacted], that she wanted to know if there were any restrictions on teleworking outside of the US from the countries of India, China, Pakistan and Africa. A day later, [redacted], in an email, asked [redacted], AITC [redacted], and two [redacted] VA ISOs, "Are there any restrictions on teleworking outside of the US?" He said that he looked in VA's teleworking policies and other VA documents and that he did not find anything that restricted teleworking while traveling internationally. (b)(6)

In a January 25, 2013, follow up email to [redacted], with [redacted] and [redacted], AITC [redacted], on copy, [redacted] said, "I have not heard anything further so I'm assuming teleworking from other countries is acceptable…We have an individual planning to travel soon and wants to insure they will be in compliance with VA rules." [redacted] responded, "Actually, Teleworking from outside the US is not allowed." [redacted] replied, "Do we have any documents or policies that state it? Also if it is not allowed, we will need broad awareness made organizationally as we have it already happening in multiple areas throughout the organization."

[redacted] told us that she was certain that there was a policy supporting her statement to [redacted]; however, no such policy was found. [redacted] told us that he believed that [redacted]' comment about a prohibition from teleworking internationally was based on an earlier response he gave when someone inquired in November 2012 about remote access from Taiwan and China. He said, at that time, he advised against the activity, because he felt that the risk outweighed the benefit. He also said that there was a lack of justification for that individual to work from an international location. (b)(6)

- In a November 15, 2012, email, Subject: OCONUS remote connections, [redacted] told [redacted], Data Center Support Division (DCSD), "*My take on it is still YES, they shouldn't do it. The risk of keyloggers and compromised credentials seems like it would outweigh the benefits…*" (Italic emphasis added.) (b)(6)

- In another November 15, 2012, email, Subject: VPN from Taiwan, [redacted] told [redacted] and others, "VA personnel cannot use RESCUE as Cisco IPSec VPN client software cannot be taken to foreign countries. In addition, US-CERT dictates IP ranges of foreign countries that are blocked for security. *CAG also has inherent risks which generally outweigh the benefits to allowing connections from foreign countries.* Based on these reasons and guidance from NSOC, I would not concur with asking or allowing personnel to connect using VA credentials from foreign countries." (Italic emphasis added.)

(b)(6)

- In a January 26, 2013, email, Subject: Foreign Telework/Security Risk Question, [redacted], IT Field Security Service, told [redacted], "Tremendous risk of compromised hardware over there. From what I have read, it is not uncommon to have laptops physically compromised while staying in hotels with Americans being targets of industrial sabotage. I can only imagine the risk to a U.S. Government employee. I would caution him to turn off wi-fi on his cellphone. I would check the State Department link on foreign travel." [redacted] forwarded the email to [redacted], who replied, "Thanks…it'll all be personal gear, so the risk is his alone."

In a January 26, 2013, email, Subject: Travel to China, [redacted] told [redacted] and [redacted], "There was a very unfortunate death event to one of my very close relatives and family friend in China recently and also my father has experienced serious health issue. Because of these, I suddenly have a very strong desire of going back to China to visit them after [redacted] years separation (my last visit was [redacted] I have told [redacted] my thoughts, seeking her help on exploring with VA Security the possibility of my teleworking from China while I am there." However, [redacted]'s flight itinerary reflected that he bought his airline ticket on October 3, 2012, over 3 months prior to asking to telework as the result of his "sudden" desire to visit China. His itinerary further reflected, and he confirmed for us, that he arrived in Shanghai-Pudong, China, on January 27, 2013, and returned to the US on February 19, 2013.

[redacted] told us that the discrepancy in his purchase of the airline ticket in October 2012 for travel in January 2013 and telling [redacted] that he "suddenly" had a "strong desire" to travel to China was that he "always plann[ed] earlier rather than waiting till the last minute." He said that he could not afford waiting until the last minute, as the cost of his flight would then be too expensive. He also said that when he booked the flight, he was not "100% sure" if he was able to travel on that date , as he needed to first decide whether he would take unpaid leave for the travel or get approval from his manager to telework while in China. In another January 27, 2013, email, [redacted] told [redacted] and [redacted] that he would take vacation if his telework from China was not approved.

(b)(6)

[redacted] and [redacted] confirmed for us that [redacted]'s travel costs were personal in nature and not billed to the task order. [redacted] told us that while in China, he did not work the first 3 days, as no one at VA had yet made a decision as to whether he could telework.

[redacted] told us that a distinction did not exist in the task order between teleworking from the continental US (CONUS) or outside the continental US (OCONUS). [redacted]'s monthly status reports and invoice records confirmed that while in China he claimed billable hours for January-February 2013. (b)(6)

[redacted] told us that there was no language integrated into the task order that allowed [redacted] to telework from China, but she said, "Why not? I've teleworked from Germany and Costa Rica." She said that she sought guidance from security and her senior management to ascertain if anything prohibited someone from teleworking from China. [redacted] told us that [redacted] asked him if a security problem existed, and he said that he could not find a security problem with [redacted] teleworking from China. However, when asked why he would not concur with someone teleworking internationally in November 2012 but saw no security risk with [redacted] teleworking from China, [redacted] told us that his personal opinion never changed. He said that he was asked "specifically for policy guidance on the topic" and when he could not find such a policy, he raised the issue to a "higher authority" in his "chain of command," which was [redacted] and [redacted], and possibly others. He said that although he was "uncomfortable with the risk/benefit balance," there was no "policy justification beyond [his] personal opinion, just gut feeling and opinion." He further said that [redacted] "appeared comfortable" with the situation, and he received no feedback from [redacted] or [redacted] as to any "potential prohibitions or problems" with the telework request. Moreover, he said that [redacted] was [redacted]'s supervisor, and it remained her authority, her decision, to allow or prohibit the telework.

[redacted] told us that [redacted] consulted with him about [redacted]'s China telework plans. He said that because he found no policy prohibiting it, he did not tell [redacted] that [redacted] was forbidden to telework from China. He said that prior to [redacted]'s departure for China, he consulted with [redacted] and he came to the same conclusion that no policy prohibited someone from teleworking from China. Mr. Warren told us that "policies and directives are the boundaries of the road. There is a lot of space between those lines that you need to transit through. So you have got to figure out what is the judgment value in terms of how do you progress within the boundaries. But there is more than just what the directives tell you. You have got to put some judgment into it." (b)(6)

[redacted] told us that VA security spent weeks researching whether policy prohibited teleworking while in China; however, security did not find any prohibitions. He said that he did not believe there was any wrongdoing, as both he and [redacted] acted on guidance approved by VA security. [redacted] said that he preferred [redacted] not telework from China, but he could not find anything in Federal or VA policy that prohibited it. However, he said that if he definitively said that [redacted] could not telework from China, most likely, it would not have happened. Moreover, he said that any of the individuals involved with [redacted]'s China telework approval process could have put a stop to it, if they felt that was the thing to do. The following VA employees told us: (b)(6)

- [redacted] said, in her opinion, China was a threat to the US, based on the news and current events.

- [redacted] said that when [redacted] approached him about teleworking from China, his first thought remained that China was considered a socialist, communist state. (b)(6)

- [redacted] said that prior to [redacted]'s departure for China, he remained aware of the potential risks posed by China. With that in mind, he said it boiled down to the determination of how much risk was too much, and what's the level where you said no, that's too much risk. He acknowledged that China caused him concern and recognized that China completely controlled their networks. Although CAG sessions remained encrypted, he said the biggest risk remained whether a Trojan—defined by an open source as a program designed to appear innocent but intentionally designed to cause some malicious activity or to provide a backdoor to a system—or Keylogger—defined by an open source as an action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard remained unaware that their actions were being monitored—existed on the CAG user's computer.

- [redacted] said that China stood as a "bad network" by those in the IT security community, and based on her knowledge of China's network, China monitored all incoming and outgoing internet traffic. She said that there remained a possibility that VA data, to include [redacted]'s username and passwords could be compromised.

- [redacted], VA Enterprise Network Defense for NSOC, said that while in China, an individual in some way, shape, or form accessed a network controlled by a company in China or the Chinese government. He said that the information going across that network may well be susceptible to exposure.

- [redacted] said that he considered China a threat to VA operations, because he knew about its practices and the hacking of US entities. He said that accessing VA's network from a different country raises issues such as the Internet Protocol (IP) being traced to VA's network, and the use of Keylogger applications, which could be used to determine a username and password. (b)(6)

- [redacted] said that in regards to CAG and malware risk, the only risk that existed would be Keylogger, which was why he asked that [redacted] change his password upon his return.

- VA OIG's ISO told us that in his "professional opinion, any traffic originating from sophisticated threat sites such as China or high threat-traffic sites like India should be outright blocked."

[redacted] acknowledged that his request to telework from China was a matter of personal convenience, but he said that it would have caused an inconvenience for VA if he could not telework, since he was the only one available to perform certain tasks on certain days. He said that if his telework request was not approved, he would have taken unpaid vacation time for this travel. [redacted] told us that she could not explain a VA business case for [redacted] to work from China and that his teleworking from China appeared to be a matter of convenience for [redacted] versus a VA business case. Mr. Warren told us that he stood hard-pressed to think that it remained a good idea for anyone to allow a VA contractor to remotely access VA networks from China. He said that he did not know why [redacted] working remotely while in China was seen as prudent or acceptable practice and that he (Mr. Warren) would not have made the same decision. (b)(6)

In a January 29, 2013, email, Subject: Direct VA Gateway Access from China, [redacted] told [redacted] and [redacted], "I just authenticated through VA Citrix side and then RDP [Remote Desktop Protocol] to my VA desktop briefly between 8:30pm and now (and may try a little more later). It is a lot faster than [if] I RDP to my home computer in Michigan first then from there authenticate to the same Citrix side and RDP to my VA desktop." [redacted] said, "I will be taking tonight off as no formal approval from VA yet." In a follow-up email, [redacted] told [redacted], [redacted] was able to perform the test–successfully able to login through CAG."

In an email 2 days later, [redacted] asked [redacted], "Any word on the working from China? I sent you the test results two days ago–he can access through CAG." [redacted] replied, "No Ma'am. Still no response. Based on multiple tries, I say let's proceed." In a February 1, 2013 email, Subject: Approval to TW, [redacted] told [redacted], "I just received approval for you to TW from China." (b)(6)

[redacted] told us that prior to traveling to China he purchased a laptop from an electronics store located in the US. He said that he did not install VA approved software, such as antivirus protection or firewall with a VA-approved configuration, as required by VA's SMS task order and VA policy. He said that he used the standard software and default setting that came with Microsoft Windows 8. He also said that the computer was not encrypted with FIPS 140-2 validated encryption, which was required by the task order. [redacted] told us that he used the computer daily to access the internet, email, etc., and that he logged into CAG via the internet, remotely connected to his VA-issued computer located in Austin (AITC), and then connected from that computer to VA's network. He said that he obtained internet access from the local area connection at his parents' house or a wireless card. He told us that he purchased the wireless card from a store in China, using it for internet access, as it was faster and more stable than the connection at his parents' house.

[redacted] told us that he had administrator access to all the AITC Unix and Linux servers, and this access included Veterans Benefit Administration (VBA) Data Warehouse (VD2); VBA Corporate Applications (CRP); VBA Corporate Web Environment (WBT); Health

Data Repository (HDR); Loan Guaranty Service (LGY); and My HealtheVet (MHV). He said that his responsibility as a VA contractor employee was to ensure that the servers were up and running and he denied having access to any personal identifying information contained within these systems.

[redacted] told us that he did not sanitize the hard drive of the personal computer he left in China, as required by VA's SMS task order, prior to returning to the US. He said that he reimaged it when he installed Windows 7 on it and that he installed Windows 7 because his family member disliked Windows 8. We found many websites reflecting that data on a computer was still accessible even after being reimaged, and we found websites offering free, or at a minimal cost, software to restore that data. Since appropriate security measures were not taken, the COR, CO, the project manager, and ISO could not verify that [redacted] met all security requirements, as per VA policy, prior to leaving the computer in China. Both [redacted] and [redacted] told us that they were not aware, nor told of, [redacted]'s request and plan to work from China, prior to his departure or while he was teleworking from China; however, VA's SMS task order required that the CO, COR, project manager, and ISO be notified of a contractor using non-VA equipment and to verify that all security requirements were met. (b)(6)

[redacted] initially told us that he only used CAG to connect to VA's network; however, his activity logs reflected that he also accessed VA's network using RESCUE-GFE on January 27 and February 3, 10, and 17, 2013. He later told us that he accessed the network using RESCUE-GFE through the VA-issued computer located at his home to access the Primavera application to submit his weekly timesheets. He denied accessing any other systems while using this method to connect to VA's network, and we were unable to confirm his assertions, due to the passage of time and unavailability of records.

Chinese Police Incident

[redacted] told us that a few days after we interviewed him, about 1 year after his trip to China, local Chinese police called his brother to elicit information about [redacted] and his extended family. The police wanted to know how often [redacted] traveled to China, but [redacted] said that his brother knew little about his activities except that [redacted] lived and worked in the US. He said that his brother told him the police wanted the information for census purposes. Open source material reflected that Shanghai's police were responsible to keep the peace in local neighborhood and business districts and "maintained records on the households and inhabitants in geographic areas. Traditionally, these so-called 'census police' worked closely with neighborhood committees and work groups. Residents stood required by law to inform the police if they took in a boarder, perhaps a family member from another town, and to let the police know if they planned to leave the city." (b)(6)

The US State Department travel website reflected that Chinese security personnel carefully watch foreign visitors and may place them under surveillance. Hotel rooms, offices, cars, taxis, telephone, internet usage, and faxes may be monitored onsite or

remotely, and personal possessions in hotel rooms, including computers, may be searched without a visitor's consent or knowledge. Business travelers should be mindful that trade secrets, negotiating positions, and other business-sensitive information may be taken and shared. http://travel.state.gov/content/passports/english/country/china.html.

Improper Teleworking from India

In an April 16, 2013, email, Subject: Request for remote work for [redacted], [redacted] told [redacted] and [redacted], "I have [a] few short but important personal works came up in India that are pending due to me being half way around the globe for almost 3 years and they are requiring me to be in person now. Also it is time for my VISA renewal." In his email, [redacted] requested to work remotely from India from May 5 to June 21, 2013. The next day, [redacted] replied, "Approved." [redacted] replied, "In this case the contractor is a TEK employee, and both TEK and the VA are OK with him working from India for several weeks." (b)(6)

Although [redacted] submitted a request to telework from New York a year earlier, during the May and June 2012 time period, he told us that he did not submit a request to telework from India from May to June 2013. He said that while in India he worked from May 6 to June 3 and that he took sick leave June 4–15, 2013. He also said that he stayed with and worked from his parents' home; he used CAG to connect to VA's network; and he used a personally-owned laptop that he brought with him to India from the US.

[redacted] told us that [redacted] and [redacted] approved his request to work from India; however, [redacted] told us that his "approval" served as concurrence for [redacted] to be absent during the proposed time period based on workload and was the first step in a process that led to final approval by the contracting office. [redacted] said that the COR and VA security approved [redacted]'s remote work from outside the US. [redacted] told us that his approval decision was based on the authority that he believed he possessed as a [redacted] and that during the weeks that led up to [redacted] leaving for India, he spoke with [redacted] about it. He further said that as an intermediary, [redacted] disclosed that [redacted] reported that VA did not have any objection to [redacted]'s travel plans, as long as [redacted] did not take GFE with him. [redacted] told us that he felt reassured about [redacted] working remotely from India, since [redacted] did not object. [redacted] further said that he took VA's concurrence to mean that VA did not perceive much risk associated with [redacted] working form India.

[redacted] told us that the SMS program office specifically asked him about the matter, but he said that VA security personnel broached the question as to whether an individual could use CAG while outside the US. He said that on that question, they determined that prohibitions did not exist. [redacted] further said that they sought guidance from the CO, the Office of General Counsel (OGC), and the Office of Cyber Security (OCS), and OCS (b)(6)

found no prohibitions on using CAG from an international location. [redacted] then questioned why OIG was conducting an investigation, if there was "no prohibition on accessing the VA network through the use of CAG outside the United States."

In an April 17, 2013, email, [redacted], SMS [redacted], asked [redacted], "Is there any policy or criteria that prevents contractors accessing the VA network or working from India?" [redacted] replied, "The last person was not allowed to take any equipment [GFE], but there was no policy saying they couldn't access the CAG from anywhere in the world. I'm thinking same situation, equipment needs to stay here, but unless we put out some policy, no reason why they couldn't use CAG from over there." (b)(6)

In an April 18, 2013, email, Subject: FW: Request for remote work for [redacted], [redacted] asked [redacted], "Is this allowed under the DCAT4 contract?" [redacted] replied to [redacted] and [redacted] that remote work was authorized under DCAT4 but that he was uncertain about whether the work had to be performed solely within the US. He asked [redacted] if she was aware of any prohibitions from a contractual perspective for work to be performed on foreign soil. [redacted] then replied to [redacted], with [redacted] on copy, "Last time this popped up, the individual was allowed to work from the other country, but they had to use CAG for access and were not allowed to take a laptop. There is still risk that way, but it is lessened."

In an April 18, 2013, email, Subject: Re: Request for remote work for [redacted], Mr. Gary Stevens, VA Director of Cyber Security, told [redacted], "We should not authorize this action. Why is the contractor traveling to India with a VA laptop?"

In an April 18, 2013 email, [redacted], VA OSC Security Reports & Oversight Management-Policy and Governance Team, told [redacted], [redacted], and others that she asked OGC "several years ago" whether it was "technically and procedurally possible to provide non-US citizens access from outside of the US to VA computers." In her email, she provided them the OGC attorney's response:

> I don't know of any law or regulation that prohibits us from granting access to VA information and information systems to non-citizens, whether they're within the U.S. or not. Absent a specific prohibition, providing access is generally at our discretion (although there are some exceptions). Since VA is, in those cases, permitted but not required to make such disclosures, we can control access to VA information through policy.

[redacted] then asked the attorney, "So, as there is no statutory law against providing access to non-citizens in a foreign country to our VA information and resources and our current VA security policy doesn't specifically prohibit it, then it can be done and should (b)(6)

be looked at on a case by case basis? If we decide to prohibit it in the future version of 6500 Handbook, we can do so without issue?" The attorney replied:

> You're correct; VA may consider the issue on a case-by-case basis and may revise agency policy to address this issue. There's no legal authority at the moment that specifically prohibits access to non-citizens outside the country. *[Federal Information Security Management Act], however, requires agencies to enforce technical, physical, and administrative requirements on vendors, and this would clearly be difficult with vendors overseas.* I would therefore agree with your recommendation. (Italicized emphasis added.)

A short time later, [redacted] responded to [redacted], [redacted], and others, "So, we are back to nothing prohibits it via policy or legally. Not excited about it, but I guess my preference is to allow the work via CAG, but not allow the devices to travel. Is that the consensus?" (b)(6)

In an April 22, 2013, email, [redacted] told [redacted], VA Contract Attorney, [redacted], [redacted], and others that her concern remained about remote access outside of the US and that she was "honestly not familiar with such requests and not sure if we should be concerned any further in regard to the remote access being outside the U.S….SMS would have to provide assurances the resource has followed and completed all necessary documentation before access is given."

In an April 29, 2013, email, [redacted] told [redacted], "The security POC has verified through Office of Cyber Security that OCONUS access is allowed by policy…I do not think India is on the list of enemy countries…this was where I was kind of going with the question?" [redacted] replied, "PWS does allow for remote access as long as *all restrictions/security requirements are being complied with*. If we have something on record from the Office of Cyber Security that this type of OCONUS-requested access is permissible, I would think that we are clear." (Italicized emphasis added.)

In an April 29, 2013, email, [redacted] told [redacted] and others, "I've confirmed with Office of Cyber Security that VA policy allows it. Even though now that they are aware that policy allows it, they may change the policy soon."

[redacted] told us that she recalled being asked to provide an opinion about [redacted] remotely working from India and that the PWS allowed for remote access as long as all the restrictions and security requirements were met. However, [redacted] said that she requested OCS provide their insight and they disclosed that VA policy did not restrict this type of arrangement. [redacted] told us that she provided an opinion on the matter; however, she provided no reason to say [redacted] absolutely could not work remotely from India. She further said that during all the discussions about (b)(6)

[redacted] working remotely from India, she never inquired about the VA business case for his request to work from an international location, and said, "I should have. I would agree I probably should have, yes."

In an April 30, 2013, email, [redacted] told Mr. Stevens and others, "Okay, so finally got word back from contracting and legal officially. No issues on that side. From below, no issues on policy side. We are right back where we started. So, do I allow this with equipment? Only other option is to force no equipment to travel and that CAG be used." (b)(6)

In an April 30, 2013, email, Subject: Work from India, [redacted] told [redacted] and [redacted], "Good news. Contracting is OK with the work from India arrangement. HOWEVER, they asked that you bring your GFE in to the AITC and leave it here during your time overseas."

In an April 30, 2013, email, Mr. Stevens told [redacted], "This request, as well as the prior request for the user to remote in from China has revealed a significant policy gap at the VA." [redacted] replied, "I understand Gary's [Stevens] perspective, but unless someone says definitely no for some justifiable reason, we are moving forward with the CAG only access. Laptop and bberry are getting locked up at AITC." He also said that he fully supported changing VA's policy immediately.

[redacted] told us that his trip to India was for personal business but that he believed there was also a VA business case. He said that if he took vacation, his work would be unnecessarily delayed for 30-45 days. [redacted] told us that it remained more cost effective to allow contractor employees to continue to work, since their duties were receptive to being performed under a telework situation or remote access. [redacted] told us that [redacted] was the primary resource for WebLogic administration for several projects and that to have him inaccessible for an extended period of time could have caused a difficult situation in terms of support. [redacted] told us that SMS had quite a few employees who are citizens of India and that they returned to India every couple of years. He said the trips were a hardship for these employees, and it was more convenient for SMS, since they did not lose the coverage of that employee for a long period of time.

[redacted] told us that prior to traveling to India he did not install VA approved software, such as antivirus protection or firewall with a VA-approved configuration, as required by (b)(6)
VA's SMS task order and VA policy. He also said that he did not ensure that his computer was encrypted with FIPS 140-2 validated encryption as required by the task order. [redacted] told us that he used this computer a "couple of times" to access VA networks prior to his travel to India and that he used it "Daily. Daily. 5 days a week, except for the last 2 weeks (June 4th to 15th)" while in India to access the internet and for teleworking by using a local area connection. [redacted] said that no one at VA inspected his computer, after he returned to the US; his computer hard drive was not sanitized; and he did not change his passwords once he returned to the US. He also said that he used his

computer to access VA networks since returning to the US and that he still had possession of the computer. Since appropriate security measures were not taken, the COR, CO, the project manager, and ISO could not verify that [redacted] met all security requirements, as per VA policy.

(b)(6)

OIG Hotline Referral to VA NSOC

On February 19, 2013, VA OIG Hotline referred to Mr. Killian an allegation that [redacted] and [redacted] improperly approved for [redacted] to telework from China from January 29 to February 17, 2013. They told him that he needed to determine the merit of each allegation, to include how each allegation was reviewed, whether they were substantiated, what corrective action was taken, when he initiated or completed that action, and the value of any recoveries or savings, as requested in the initial referral.

In an April 25, 2013, email, Subject: RE: VA OIG Hotline Referral Case No. 2013-01730-HL-0432; Austin Datacenter Austin, TX; RP71, Mr. Stevens asked Mr. Killian, "What is the business case for a person to operate from China, especially given the fact they will be connecting to the VA from a Chinese connection?" Mr. Killian replied, "From my perspective, I would prefer the connection not take place but the business justification is with the supervisor/COR. The caveat would be we are not responsible for any loss of or incomplete work due to blocks being implemented for the sake of securing the enterprise."

On April 26, 2013, Mr. Killian told VA OIG Hotline, "In researching this issue, I have concluded: 1) the contractor noted in the allegation is currently employed by VA; 2) the contractor is authorized to use remote access technologies; 3) there have only been connections from domestic addresses; 4) telework arrangements occur between an employee and a supervisor. OIG Hotline replied to Mr. Killian and told him that his response was incomplete.

In a May 9, 2013, memorandum, Mr. Killian told VA OIG Hotline:

- In researching the alleged security violation, it is substantiated that [redacted] provided approval for [redacted] to telework from China.
- During review, it was determined: (b)(6)
  - [redacted] has an approved telework agreement with supervisor [redacted]
  - [redacted] had a modified telework agreement approved by [redacted] for the period of January 29, 2013, through February 17, 2013

- The remote access account assigned to [redacted] was logged into and connected from IP Addresses assigned to China several times from the period of January 30, 2013, through February 17, 2013

- While the elements of the allegation prove to be substantiated, the actions taken by the supervisor and the employee were not in violation of security policy.

  - In accordance with VA Directive 5011, telework agreements are established between the employee and the supervisor to provide alternatives to the traditional worksite in accomplishing work objectives. The attached telework agreements substantiated the ability for the employee to telework.

  - As evidenced by the attached telework agreement, the employee was authorized to telework from China.

  - VA does not prohibit remote connections from locations outside of the US.

  - Due to inherent security risks, some IP address ranges are blocked; however, the addresses the employee connected from while in China are not blocked.

(b)(6)

Mr. Killian told us that he sent the VA OIG Hotline referral to [redacted] with several questions to address the allegations. He said that when he initially responded to VA OIG Hotline, he believed that he had all the relevant information. He further said that he put too much faith in [redacted] and that he (Mr. Killian) should have put more of an effort into it. He said that in hindsight, he would probably talk to the actual supervisor, instead of going on second-hand information and/or collecting artifacts from someone else. Mr. Killian told us that during his review, he did not recall asking why [redacted] traveled to China, as he did not think it was within his scope of responsibility. We found that Mr. Killian's submission to the VA OIG Hotline did not reference any forensic examinations of VA's network subsequent to [redacted]'s international activity. Mr. Killian told us that he did not instruct anyone to perform a forensic exam of VA's network, as the network was huge and to conduct forensics on it was impossible.

Mr. Warren told us that in the fall of 2013, he learned of a VA OIG Hotline complaint that referenced two contractor employees, [redacted] and [redacted], doing system administration work "offshore" from China and India. He said that he then directed that such activity cease and to discontinue the practice. He further said that the response he received was that VA Handbook 6500 did not prohibit the practice, and he reiterated "that practice needs to cease." He, however, said that he did not instruct anyone to do a forensics examination of the network, as his focus was on stopping the remote access to the network while determining "what the rules should be," given the information that there was nothing in the policy that prohibited it. He also said that he did not want to

(b)(6)

interfere with any OIG work being done; however contrary to his assertion, OIG Hotline referred this matter to Mr. Killian to investigate and address in early February 2013.

In a December 2, 2013, email, Subject: INFO – OIS Staff Call – 12/2/13, Mr. Randy Ledsome, Director of Field Security Service, told [redacted], Mr. Stevens, and others that they discussed two policy issues.

- Prohibit the usage/manipulation of VA data on personal home computers unless utilizing CAG. CAG doesn't allow data to be stored locally on a computer.
- Prohibit remote access from non-NATO countries

Mr. Ledsome then asked, "Can you provide the recommended 6500 [VA information security policy] language to share with Stan [Lowe]?" (b)(6)

In a response email 10 minutes later, Mr. Stevens asked Mr. Ledsome, [redacted], and others, "Instead of just providing the language, can you develop two policy memos for signature by Mr. Warren?"

Mr. Lowe told us that he first learned of the remote access to VA's network from outside the US in late fall or early winter 2013 when Mr. Warren asked him to participate in a telephone conversation between Mr. Warren and an unrecalled individual. He said that Mr. Warren asked him (Mr. Lowe) to clarify VA policy and whether VA policy prohibited employees accessing VA's network via VPN from outside the US. Mr. Lowe said that either that same day, or within the next week, he instructed Mr. Killian to shut down remote access from outside the US. However, he said that he did not recall any temporary order or memorandum being issued to field employees instructing them to cease and desist the offshore practice. He further said that it took 2-3 months to get the memorandum drafted, which served as policy, stating that remote access to VA's network was prohibited from non-NATO countries. He explained that it took so long to get the memorandum in place, because it had to be "vetted through the system." He said that was how VA accomplished policy change or clarification with regards to information technology resources, as everyone was "hypersensitive" about ensuring they did not do anything that caused harm to patients or impacted mission delivery.

A January 15, 2014, Memorandum, Subject: Remote Access, signed by Mr. Lowe, stated:

> 1. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program Policy* requires the use of a VA approved method to connect external systems to VA's network. CAG is the current VA approved method for users when they must use or manipulate VA information for official VA business. CAG authorized

> users are not permitted to print or save VA information to their personal computers.
>
> 2. In addition, VA prohibits access to VA's network from non-NATO countries. The exception to this are countries where VA has approved operations established (e.g., Philippines and South Korea).

A May 29, 2014, VA OIG Office of Audits & Evaluations report (13-01391-72), titled: *Federal Information Security Management Act Audit for Fiscal Year 2013*, confirmed that the non-NATO countries requirement was formalized in the current draft version of VA Handbook 6500 that stood to be published by the end of fiscal year 2014. It further reflected that OIT began blocking top level domains for country codes and IP addresses for countries that may pose a significant security risk to VA systems.

A February 4, 2014, Memorandum, Subject: Connection to VA Information Systems Using Personally Owned Equipment (POE), signed by Mr. Lowe, stated:

> 1. VA Handbook 6500 establishes the foundation for [VA] comprehensive information security program and its practices, based on the National Institute of Standards and Technology (NIST) and provides the minimum mandatory security control standards for implementation of VA Directive 6500, *Managing Information Security Risk: VA Information Security Program.* The Handbook applies to all VA Administration and Staff Offices and pertains to all VA information which is stored, generated, transmitted or exchanged by VA employees, contractors, subcontractors or a third party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf.
>
> 2. VA provides [CAG] for remote access to the VA Network for business needs. CAG is a secure application and data access solution that provides strong security while empowering users with remote access.
>
> 3. CAG is the only authorized VA Network connection client for [POE]. POE is not authorized to utilize any other access method and is prohibited from use on the VA network.

We interviewed Mr. Warren on February 4, 2014, concerning the allegations of VA contractor employees accessing VA's network from foreign countries. Once we learned that OIT information security employees had not yet performed an assessment or forensics of VA's network to determine if there was any compromise to the system or VA data, we asked Mr. Warren to ensure that a risk assessment and forensics be conducted. He told us that this situation required more than a forensics question of [redacted] (b)(6)

[redacted] access but what rights did he have, what system did he have rights to, what information was on those systems, and with the rights he had, could he access those systems. He further said that there were "a lot of open questions from a risk standpoint that needed to be answered…The analysis will tell us if actually something untoward happened." (b)(6)

In a February 5, 2014, email, Subject: Analysis of potential risk based on a specific set of conditions that existed last year, Importance: High, Mr. Warren told Mr. Lowe and Mr. Art Gonzalez, Deputy Chief Information Officer, with Ms. Martha Orr, Executive Director of Quality, Performance and Oversight, on copy:

> I have been made aware of two specific instances of individuals who accessed VA systems in a manner that may have introduced increased risk to VA.
>
> I would like a risk/impact analysis to be accomplished to determine, as best as we are able, what level of risk was taken on by the VA and if there was a likely exposure of data[.]
>
> 1. Identify what systems the individuals had enhanced access to[;] 2. Determine the type of enhanced access[;] 3. Determine what data or systems could have been at risk as a result of that enhanced access[;] 4. Based on 1-3 perform a detailed analysis on those systems[;] 5. Based on 1-3 and date ranges [included below] perform a detailed analysis of the logs for those systems[;] 6. Based on 1-3 and date ranges [included below] perform a detailed analysis of the logs for our defense in depth sensors or devices that align with those systems[;] 7. Based on the date ranges [included below] review logs on traffic with our external partners[;] 8. Add additional analysis or forensics steps (if any) your SMEs recommend[.] Based on the above looking for an evaluation of events monitored or identified to determine whether the activity was within the bounds of normal for the duties of these two individuals had or if there was a likely exposure of VA data. Looking for a data driven report.

OIT NSOC final and supplemental reports (VANSOC0603474), dated April 2, 2014, and May 22, 2014, as well as a separate spreadsheet, appeared as though the VA-NSOC Digital Forensics Team conducted a very limited analysis and did not fully address the items outlined in Mr. Warren's February 5 email. The reports reflected that the analysis objective was to "analyze web history for each machine during the time reported that the machine's user logged in internationally." It further reflected that the audit of logins found only five users logged in internationally during the specified time periods. They analyzed six VA-issued computers, of which none were assigned to [redacted] or [redacted], and no personal computers were examined. A March 25, 2008, OGC memorandum (b)(6)

stated that VA could search and seize personally-owned electronic equipment under identified circumstances. VAOPGCADV 5-2008.

The reports reflected that from login records they determined that five users logged in internationally. Of those five, one machine had web activity during international login to a bank, and three were confirmed to have been used during the respective time periods. A separate spreadsheet reflected 30 contractor employees, the name of their respective employer, what access they had to VA systems, and whether each accessed VA's network from an international location. The spreadsheet identified seven contractor employees who accessed VA's network from an international location using either CAG or VPN to log onto the network.

In a December 17, 2014, email, Ms. Orr told us that OIT gave us "all of the information" generated by OIT's risk analysis of VA's network as a result of Mr. Warren's February 5, 2014, email and that she "validated" through Mr. Lowe that there was nothing further.

Unauthorized International Teleworking

[redacted] told us that as a VA employee and while on personal travel, she used GFE to telework from Costa Rica in October 2011 and in the 2011-2012 and 2012-2013 winter months from Germany. She said that she also took her GFE to Great Britain in November 2011, but she was unable to connect to VA's network. She said that she took her GFE with her on a Caribbean cruise in February 2012, and she used a VA-issued broadband card to telework. Although she took annual leave for her personal travel, she said, "Wherever I travel, I bring my laptop and my Blackberry and I work." [redacted] told us that she did not notify her VA supervisor, local CIO, and ISO that she was taking her VA-issued laptop and Blackberry with her while on personal international travel; however, VA policy requires an employee to notify these individuals so that appropriate actions can be taken prior to departure and upon return. She further said that she used VPN to connect to VA's network while on international personal travel. (b)(6)

Improper Access of VA's Network from Foreign Countries

[redacted], [redacted], and [redacted] identified additional VA contractor employees who accessed VA networks from foreign countries. On February 19, 2014, we provided this list of names to Mr. Warren so that OIT employees could add them to their forensic examination of VA's network to identify any security risks. Based on testimony, logs we pulled, information provided to us in the OIT April and May 2014 reports, as well as the separate OIT spreadsheet, we determined that the following individuals improperly accessed VA networks from foreign countries: (b)(6)

- [redacted] – unknown citizenship – Traveled to India September 24-28, 2013. Log activity reports reflected CAG activity during this period. The OIT final forensics reports and spreadsheet provided no information about access activity.

(b)(6)

- [redacted] – a citizen of India – Traveled to Canada November 1-4, 2013. Log activity reports reflected CAG activity during this period. The OIT final forensics reports and spreadsheet provided no information about access activity.

- [redacted] – a citizen of India – Traveled to Canada October 2-11, 2013. Log activity reports reflected CAG activity during this period. The OIT final forensics reports and spreadsheet reflected that VA's network was accessed through CAG from Canada in October 2013; however, there was no evidence that a VA-issued computer was used to gain this access.

- [redacted] – a citizen of India – Traveled to India April 1-30, 2013. Log activity reports reflected RESCUE-GFE and CAG activity on April 18, 2013. The April 2014 OIT final forensics report and spreadsheet reflected that VA's network was accessed by use of VPN with an international login from India on April 18, 2013, at 06:33:08; however the report also reflected an inability to confirm account activity, since the security event log no longer kept data from April 2013.

- [redacted] – unknown citizenship – Traveled to India November 30–December 16, 2013. Log activity reports reflected CAG activity during this period. [redacted] identified [redacted] as [redacted], who also worked as a VA contractor employee. The OIT final forensics reports and spreadsheet provided no information about access activity.

(b)(6)

- [redacted] – former citizen of China and a dual citizen of Canada and US – Traveled to China January 27 to February 19, 2013. Log activity reports reflected RESCUE-GFE and CAG activity during this period. The OIT final forensics reports and spreadsheet contained no information identifiable with [redacted]

- [redacted] – a citizen of India – Traveled to India November 11–December 19, 2011; July 2–30, 2012; and August 3–27, 2013. Log activity reports reflected no activity in November–December 2011 or July 2012, but reflected CAG activity in August 2013. The OIT final forensics reports and spreadsheet provided no information about access activity.

(b)(6)

- [redacted] – a US citizen – [redacted] told us that she accessed VA networks while on personal travel to Costa Rica in October 2011, personal travel to Germany in the winters of 2011 and 2012, and while on a Caribbean cruise in February 2012. The OIT final forensics reports and spreadsheet provided no information about access activity.

- [redacted] – a citizen of India – Traveled to India May 5–June 16 and November 30–December 16, 2013. Log activity reports reflected CAG activity during the May–June time period, and the OIT final forensics report reflected that VA's network was accessed by a CAG international login from India during the May–June 2013 time period. Reports showed no activity in the November–December 2013 time period.

(b)(6)

- [redacted] – a citizen of Canada – Reports reflected access from an IP located in Canada during the November 2013 period. The OIT final forensics reports and spreadsheet disclosed that based on activity logs, VA's network was accessed through an international login from Canada between November 3, 2013 at 02:33:43 and November 5, 2013 at 16:31:04.

- [redacted] – a citizen of India – Traveled to Canada December 11–16, 2013. Log activity reports reflected RESCUE-GFE and CAG activity during this period. OIT final forensics reports reflected that VA's network was accessed using a VPN login and that the international login occurred from Canada between December 11, 2013 at 14:25:22 and December 15, 2013 at 19:17:26.

- [redacted] – a citizen of Jamaica – OIT spreadsheet reflected access from Jamaica using CAG in June 2013 and using VPN from Jamaica in November 2013. OIT final forensics reports reflected that an international login using VPN occurred from Jamaica on January 25, 2014 at 02:59:01.

- [redacted] – a citizen of India – Traveled to Canada April 10–15, 2013, and to India in August 19–September 7, 2013. Log activity reports reflected CAG activity and RESCUE-GFE activity during these time periods. The OIT final forensics reports reflected VA's network was accessed by a VPN login from Canada in April 2013; a CAG login from the United Arab Emirates (UAE) in July 2013; and a CAG login from India in August 2013. The report also reflected the inability to confirm account activity, since the security event log no longer kept data from April 2013 and was cleared in June 2013.

(b)(6)

- [redacted] – unknown citizenship – Traveled to India December 31, 2013 to February 3, 2014. Log activity reports reflected RESCUE-GFE and CAG activity during this period. OIT final forensics reports and spreadsheet provided no information about access activity.

- [redacted] – a citizen of India – Traveled to Canada January 27–March 1, 2013; India March 4–29, 2013; Canada April 1–4, 2013; and India November 2–8 and 25–29, 2013. Log activity reports reflected CAG activity during these time periods. OIT final forensics reports and spreadsheet provided no information about access.

[redacted] gave us a spreadsheet identifying about 300 DCAT4 contractor employees with telework agreements, and we obtained a list of over 30 contractor employees with access to VA's network as part of DCAT4 and who are not US citizens. They are from a number of foreign countries, such as India, Cameroon, Netherlands, Pakistan, Jamaica, etc. Considering the volume of potential teleworkers, it was quite possible that some of these contractors also accessed VA's network internationally. As an example, [redacted], at times, remotely logged into his VA-issued computer located within the US and then accessed VA's network. That access then appeared as if he logged into the network with an IP address within the continental US and not from China. Other contractor employees may also have first logged into computers located within the US and then gained access to VA's network so that an international IP was not detected. (b)(6)

Conclusion

We found that OIT AITC employees failed to follow VA information security policy and contract security requirements when they improperly approved a telework request and allowed [redacted] to work remotely and access VA's network from China using POE that he took to and left in China. He not only accessed VA's network from China, he at times first logged into his VA-assigned computer located in the US so that when he gained access to VA's network, VA security systems did not recognize the connection as coming from China but instead from within the US. We also found that they failed to follow VA information security policy and contract security requirements when they allowed [redacted] to work remotely and access VA's network from India using POE that he took with him to India and then brought back to the US. We also found that [redacted], as a VA employee, and other VA contractor employees improperly connected to VA's network from international locations.

We also found that OIT employees, because they did not find a specific VA policy prohibiting access to VA's network from foreign countries, even possible cyber-threat countries, would not prohibit it. Although two OIT employees voiced concerns about a VA contractor employee working from China, they were ignored. [redacted] said that it was permitted, since there was no VA policy to prohibit it, and [redacted] said that he did not find a security problem with [redacted] teleworking from China. (b)(6)

We further found that after the Acting CIO learned of this improper remote access and he gave verbal instructions for it to cease, VA information security employees at all levels failed to quickly respond to stop the practice and to conduct a forensic examination to determine if there was a risk to any VA data as a result of VA's network being accessed internationally or to mitigate or alleviate any possible compromise to the system. Mr. Warren's assertion that he did not want to take any action when he learned of the foreign remote access so as to not interfere with any efforts by OIG was not credible, as OIG Hotline initially referred this matter to those within his chain of responsibility to address in early February 2013.

In our review of 14 VA contractor employees whom we identified as accessing VA's network while traveling abroad, we found that between the time that OIG Hotline referred the initial allegation to Mr. Killian on February 19, 2013, and when the Director of Field Security Service discussed two policy issues 10 months later, 11 of the 14 VA contractor employees accessed VA's network from an international location. We also found that 3 of the 14 accessed VA's network between the time of the discussion of the two policy issues on December 2, 2013, and the issuance of the January 15, 2014, memorandum requiring the use of CAG and prohibiting access to VA's network from non-NATO countries. Furthermore, we found that 2 of the 14 accessed VA's network from a non-NATO country, after the issuance of that memorandum. Although Mr. Lowe told us that he instructed Mr. Killian to shut down remote access from outside the US in late fall or early winter 2013, we found that it continued after he gave those instructions.

Transcripts from a June 4 2013, hearing before the US House of Representatives, Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, revealed that Mr. Warren knew as early as 2010 that there were "uninvited visitors" in VA's network, one being China, who compromised or attacked it by taking advantage of "weak technical controls within the VA network." Mr. Warren said that he took any potential incident or incident seriously; however, when he learned that VA contractor employees worked remotely from China and India, his only instructions were to cease the practice, as his focus was to determine what "the rules should be" rather than was there any compromise to any VA data. Had he and other OIT employees taken a more active approach, they would have found that at least one VA OIT employee and numerous VA contractor employees improperly accessed VA's network from foreign countries on numerous occasions using both CAG and RESCUE-GFE, with one leaving the computer he used in China. They would also have found that OIT employees put more emphasis on whether there was policy prohibiting a possible cyber threat situation rather than what policies were in place to reduce or mitigate any such risks and that OIT employees responsible for oversight and to investigate and mitigate security breaches of VA's network failed to use their experience, common sense, and good judgment in regards to individuals and their international remote access to VA's network.

Moreover, after we asked that a complete forensic analysis be completed to address any possible risk and/or compromise, Mr. Warren did not ensure that the instructions he gave Mr. Lowe and Mr. Gonzalez in his February 5, 2014, email for a "risk/impact analysis" were thoroughly completed. He asked them to determine what "level of risk was taken on by the VA and if there was a likely exposure of data," yet the reports given to us appeared as though the VA-NSOC Digital Forensics Team conducted a very limited analysis and did not fully address the items outlined in Mr. Warren's instructions. Due to the passage of time and with no access to the computer [redacted] left in China, there was no way for us to determine what was contained on it or if it was still being used to remotely access VA's network. (b)(6)

Recommendation 1. We recommend that the VA Chief of Staff (COS) confer with the Offices of Human Resources (OHR), General Counsel (OGC), and Accountability Review (OAR) to determine the appropriate administrative action to take, if any, against the OIT employees involved in this particular matter.

Recommendation 2. We recommend that the COS confer with OGC and the Executive Director of the Office of Acquisition Operations (OAO) to determine the appropriate action to take against Systems Made Simple, Inc., for contractor employees failing to adhere to VA information security policies and contract security requirements.

Recommendation 3. We recommend that the COS ensure that VA's information security policies are thoroughly reviewed and rewritten to address any weaknesses.

Recommendation 4. We recommend that the COS ensure that VA's information security training is thoroughly reviewed and rewritten to address any weaknesses.

Comments

The VA Chief of Staff was responsive, and his comments are in Appendix A. We will follow up to ensure that recommendations are fully implemented.

JAMES J. O'NEILL
Assistant Inspector General for
Investigations

Appendix A

VA Chief of Staff Comments

Department of Veterans Affairs **Memorandum**

Date: March 31, 2015

From: VA Chief of Staff (00A)

Subject: **Administrative Investigation, Improper Access to VA Network by VA Contractors from Foreign Countries, OIT, Austin, TX**

To: Director, Administrative Investigations Division, VA Office of Inspector General (51Q)

This update is in response to the VA Office of Inspector General case number 2013-01730-IQ-0160.

Recommendation 1: We will confer with the Offices of Human Resources (OHR), General Counsel (OGC), and Accountability Review (OAR) to determine the appropriate administrative action to take, if any, against the OIT employees involved in this particular matter.

Recommendation 2: We will confer with OGC and the Executive Director of the Office of Acquisition Operations (OAO) to determine the appropriate action to take against Systems Made Simple, Inc., for contractor employees failing to adhere to VA information security policies and contract security requirements.

Recommendation 3: We will ensure that VA's information security policies are thoroughly reviewed and rewritten to address any weaknesses.

Recommendation 4: We will ensure that VA's information security training is thoroughly reviewed and rewritten to address any weaknesses.

If you have any question, please don't hesitate to contact me at 202-461-4831.

Jose D. Riojas

VA Chief of Staff's Comments to Office of Inspector General's Report

The following VA Chief of Staff's comments are submitted in response to the recommendation(s) in the Office of Inspector General's Report:

OIG Recommendation(s)

Recommendation 1. We recommend that the VA Chief of Staff (COS) confer with the Offices of Human Resources (OHR), General Counsel (OGC), and Accountability Review (OAR) to determine the appropriate administrative action to take, if any, against the OIT employees involved in this particular matter.

Comments: See pages 35–36.

Recommendation 2. We recommend that the COS confer with OGC and the Executive Director of the Office of Acquisition Operations (OAO) to determine the appropriate action to take against Systems Made Simple, Inc., for contractor employees failing to adhere to VA information security policies and contract security requirements.

Comments: See pages 35–36.

Recommendation 3. We recommend that the COS ensure that VA's information security policies are thoroughly reviewed and rewritten to address any weaknesses.

Comments: See pages 35–36

Recommendation 4. We recommend that the COS ensure that VA's information security training is thoroughly reviewed and rewritten to address any weaknesses.

Comments: See pages 35–36.

Appendix B

OIG Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Robert Warren (No relation to anyone named in report.)

Appendix C

Report Distribution

VA Distribution

Deputy Secretary (001)
Chief of Staff (00A)
Executive Secretariat (001B)

To Report Suspected Wrongdoing in VA Programs and Operations

Telephone: 1-800-488-8244

Email: vaoighotline@va.gov

(Hotline Information: www.va.gov/oig/hotline)