VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Unauthorized Access to VA Systems

July 27, 2011
10-03516-229

ACRONYMS AND ABBREVIATIONS

OIG	Office of Inspector General
OI&T	Office of Information and Technology
VistA	Veterans Healthcare Information Systems Technology and Architecture

To Report Suspected Wrongdoing in VA Programs and Operations:

Telephone: 1-800-488-8244

E-Mail: vaoighotline@va.gov

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

Report Highlights: Review of Alleged Unauthorized Access to VA Systems

Why We Did This Review

The Office of Inspector General evaluated the merits of a VA Hotline allegation that certain contractors, without proper security clearances, gained unauthorized access to VA systems and networks. We also evaluated whether VA was providing adequate oversight to ensure the contractor is meeting VA information security requirements.

What We Found

We substantiated the allegation that contractors did not comply with VA information security policies when accessing mission critical systems and networks. Specifically, contractor personnel: (1) improperly shared user accounts when accessing VA networks and Veterans Health Information System and Technology Architecture (VistA) systems; (2) did not readily initiate action to terminate user accounts for separated employees; and (3) did not obtain appropriate security clearances or complete security awareness training prior to gaining access to VA systems and networks.

Further, contractor systems contained a number of information security control deficiencies that could allow malicious users to gain unauthorized access to VA information systems. VA has not implemented effective oversight to ensure that contractor practices comply with its information security policies and procedures. Contractor personnel also stated they were not well aware of VA's information security requirements. As a result of these deficiencies, VA sensitive data is at risk of inappropriate disclosure or misuse.

What We Recommend

We recommend the Assistant Secretary for Information and Technology implement procedures for monitoring contractor user accounts and terminate accounts for separated employees. The Assistant Secretary should ensure contractor personnel obtain appropriate security clearances and security awareness training before accessing VA systems. The Assistant Secretary should request that the Deputy Assistant Secretary for Acquisition and Logistics modify the vendor contract to reflect higher level personnel security requirements. Further, the Assistant Secretary should review contractor system security controls and practices to ensure compliance with VA requirements.

Agency Comments

The Principal Deputy Assistant Secretary for Information and Technology agreed with our findings and recommendations. The OIG will monitor implementation of the corrective action plans.

(original signed by:)

BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We conducted this review to determine the merits of a VA Hotline allegation that certain contractors, without proper security clearances, gained unauthorized access to VA networks and Veterans Health Information System and Technology Architecture (VistA) systems at multiple VA medical facilities.

Allegation

A complainant contacted the VA Office of Inspector General (OIG) in July 2010, alleging that contractor personnel, without proper security clearances, improperly shared user accounts when accessing VA systems and networks. The complainant alleged that unauthorized access occurred at VA medical facilities in Columbia, MO; Huntington, WV; Kansas City, MO; and Wilmington, DE.

The vendor is under contract with VA to provide hardware and proprietary software offering veterans telecommunications services to remotely access VistA applications. These telephone services include refilling prescriptions and scheduling and checking future medical appointments. VistA is an enterprise-wide application used throughout the Veterans Health Administration to manage sensitive electronic health records and data.

To conduct our review, we visited the vendor's corporate offices to discuss the merits of the hotline allegation and gain an understanding of their information security controls. Further, we identified contractor employees who access VA systems and reviewed their personnel files for evidence of security clearances and security awareness training. At VA medical facilities, we reviewed VA processes for granting contractors' security clearances with related security awareness training, reviewing contractors' user accounts, and providing oversight of contractor managed systems.

Appendix A provides details on the scope and methodology of our review. Appendix B provides additional background information pertinent to our review. Appendix C provides comments by the Assistant Secretary, Office of Information and Technology, on a draft of this report.

RESULTS

Finding 1 Unauthorized Access

We substantiated the allegation of unauthorized access to VA systems and networks. We found that certain corporate officers improperly used other employees' Virtual Private Network user accounts to gain unauthorized access to VA systems and networks. During our site visit to the corporate offices, contractors admitted to sharing two of their employees' user accounts to access VA networks on a number of occasions for maintenance and monitoring of contractor systems. Further, the contractor could not provide evidence that it readily initiated actions to terminate a user account after the employee's separation date. Although the employee left employment with the contractor in May 2010, VA did not terminate the account until November 2010.

The contract with VA requires the vendor to comply with policies and procedures provided in VA Handbook 6500, *Information Security Program.* VA Handbook 6500 specifically prohibits the sharing of user accounts and requires the closing of user accounts as part of proper user account management. Further, VA Handbook 6500 requires VA personnel to regularly review user account access for inappropriate or unusual activity and take necessary actions.

Corporate officers stated they did not fully understand VA's information security requirements regarding user account access and did not believe additional user accounts were needed. These requirements were nonetheless outlined in the vendor's contract. Additionally, VA did not actively monitor user account activity or readily communicate with the contractor to identify and terminate unnecessary user accounts. Without effective controls to prevent unauthorized access by contractors, VA information systems and sensitive veteran data are vulnerable to increased risks of compromised availability, integrity, and confidentiality. The lack of individual accountability over user accounts provides ample opportunities to conceal malicious activity such as theft or misuse of veteran data.

Recommendation

1. We recommend the Assistant Secretary for Information and Technology implement procedures to ensure information security officers and systems administrators actively monitor contractor user accounts for inappropriate use and terminate accounts for separated contractor personnel on a timely basis.

Management Comments

The Principal Deputy Assistant Secretary, Office of Information and Technology, concurred with our findings and recommendation. In accordance with VA policies and procedures, the Office of Information and Technology will monitor contractor user accounts for inappropriate use. Additionally, the Contracting Officer Technical Representative will perform quarterly reviews of contractor user accounts to ensure the need for account continuation.

OIG Response

Management's comments and corrective action plans are responsive to the recommendation. We will follow up as required on all actions.

Finding 2 Security Clearances and Awareness Training

We substantiated the allegation that contractor personnel did not obtain appropriate background security clearances before gaining access to VA systems and networks. Specifically, 10 of 16 employees did not complete or could not provide evidence of background investigations. Furthermore, these same employees could not provide evidence of completed security awareness training or signed *Contractor Rules of Behavior* prior to our review.

The remaining contractor personnel had completed background investigations with a "Low" risk designation and a "National Agency Check" level of background investigation. The vendor's contract with the VA specifies a "Low" risk designation at a National Agency Check with Inquiries investigation level for contractor employees. However, VA's information policies and procedures indicate that contractor personnel, given their system-level access to VistA sensitive data at most VA facilities, should have received a "Moderate" risk designation and a "Minimum Background" level of investigation. A Minimum Background level of investigation exceeds a National Agency Check with Inquiries investigation because it includes interviews with subjects, spouses, neighbors, supervisors, coworkers, and verification of any educational degrees.

The vendor's contract with VA requires the vendor to comply with VA Handbook 6500, *Information Security Program*, which requires contractor background screening at the appropriate level, completion of security awareness training, and signed contractor rules of behavior, prior to gaining access to VA information systems. Further VA Handbook 0710, Appendix A, *Position Risk and Sensitivity Level Designation*, states that information technology positions with a Moderate risk designation level have the potential for moderate to serious impact, such as system design, operation, and maintenance, affecting large portions of VA information systems. Given a Moderate risk designation level, VA should have required a Minimum Background level of investigation for contractor personnel.

Corporate officers stated they did not fully understand VA requirements for security clearances and information security awareness training and did not believe their employees required security clearances commensurate with a "Moderate" risk designation level. Additionally, VA personnel could not provide evidence that risk assessments had been performed to determine whether the "Low" risk designation was appropriate for contractors accessing VistA systems and networks. VA needs to perform risk assessments of contractor personnel and determine whether a "Moderate" risk designation is appropriate, given the contractors' system- level access to VA sensitive data. Without effective controls over security clearances and training for contractors, VA information systems and sensitive data will be

vulnerable to increased risks by contractor personnel of unverified character and suitability.

Recommendations

2. We recommend the Assistant Secretary for Information and Technology evaluate and upgrade risk designation level for contractor personnel to "Moderate," in accordance with VA information security requirements, and ensure commensurate background investigations are performed for those personnel with access to VA systems and sensitive information.

3. We recommend the Assistant Secretary for Information and Technology request that the Deputy Assistant Secretary for Acquisition and Logistics modify the vendor's contract to increase background security requirements for contractor personnel with access to VistA mission critical systems.

4. We recommend the Assistant Secretary for Information and Technology require contractor personnel to complete initial and, as appropriate, refresher security awareness training and sign the Contractor Rules of Behavior to ensure full awareness of VA information security requirements when accessing VA systems and networks.

Management Comments

The Principal Deputy Assistant Secretary, Office of Information and Technology, concurred with our findings and recommendations. The Office of Information and Technology will request the Contracting Officer modify the vendor's contract to upgrade personnel risk designation levels to "Moderate." The Contracting Officer Technical Representative will ensure the necessary background investigations are performed for personnel working on the contract. Further, the Contracting Officer Technical Representative will ensure that contractors complete all required VA security awareness training and will retain copies of certificates from such training, as well as National Rules of Behavior and Non-Disclosure forms. By July 31, 2011, the Office of Information and Technology will send a letter reminding the contractor of its information security responsibilities and the consequences for non-compliance.

OIG Response

Management's comments and corrective action plans are responsive to the recommendations. We will follow up as required on all actions.

Finding 3 Other Security Control Deficiencies

We identified a number of information security control deficiencies during our evaluation of contractor systems at corporate offices and VA medical facilities. For the most part, these deficiencies were consistent with access control and configuration management security weaknesses identified in our Federal Information Security Management Act assessment of VA for 2010.*

Specifically, vendor systems at corporate offices contained sensitive VA data on unencrypted hard drives, allowing potential misuse or unauthorized disclosure. Vendor systems also were not formally certified and accredited to operate in accordance with VA information security policy. Compliance in these areas is imperative as contractor systems have to interconnect with mission-critical VA systems and networks to fulfill the terms of the contract. Further, contractor systems did not have adequate physical security controls, such as hardware cable locks, to protect the systems from theft.

Additionally, contractor systems at VA medical facilities did not use consistent firewall protections to prevent unauthorized access and employed unsecure network services that could allow malicious users to collect sensitive data across the VA network. Because contractor systems contained software no longer supported by vendors, the systems lacked adequate protection against virus and malware threats. VA also did not consistently implement adequate inventory controls to maintain physical accountability for the contractor's hardware, as VA policies and procedures require.

VA Handbook 6500, Appendix D, *Minimum Security Controls for VA Information Systems*, provides high-level policy for mandatory configuration settings of information technology hardware, software, and firmware; configuration of security settings for information technology products; and documentation of configuration settings. The vendor's contract mandates compliance with these VA requirements. Further, VA Handbook 6500, *Information Security Program,* requires VA Certification and Accreditation or a Contractor Security Control Assessment for contractor systems to be operational. It also requires that physical and configuration management security controls are in place. Finally, VA Handbook 7002, *Logistics Management Procedures*, requires accountability for information technology equipment at VA facilities.

VA's Office of Information Technology (OI&T) has not performed effective oversight of contractor practices to ensure the contractor is meeting VA information security requirements at vendor offices and VA medical facilities. OI&T is responsible for independently reviewing and assessing

* *Department of Veterans Affairs: Federal Information Security Management Act Assessment for 2010*, OIG Report Number 10-01916-165, May 12, 2011.

information security, privacy, records management, information physical security, specific issues and incidents, information systems, and related processes at VA facilities. Such responsibilities include performing security reviews of contractors' information security policies and practices. In October 2010 OI&T announced plans to conduct vendor site assessments that should help fulfill this responsibility. Such OI&T oversight will be key in addressing the risks that contractor systems may pose to the availability, integrity, and confidentiality of VA systems and networks.

Recommendation

5. We recommend the Assistant Secretary for Information and Technology review contractor system security controls and practices to ensure compliance with VA's information security requirements.

Management Comments

The Principal Deputy Assistant Secretary, Office of Information and Technology, concurred with our findings and recommendation. The Office of Information and Technology with contact the Contracting Officer Technical Representative and schedule a review of contractor system security controls. The target date for initiation of the system security review is July 31, 2011.

OIG Response

Management's comments and corrective action plans are responsive to the recommendation. We will follow up as required on all actions.

Appendix A Scope and Methodology

Our review determined the merits of a VA Hotline allegation that certain contractors, without proper security clearances, gained unauthorized access to VA systems and networks. To accomplish this review, we interviewed VA and contractor officials and examined the vendor's contracts with VA. We also researched applicable VA Directives and Federal information security requirements and identified relevant business processes and information system security controls.

We evaluated VA business processes for providing contractor security awareness training, background clearances, and access to VA systems and networks. We also assessed VA activities to monitor contractor user accounts for active and separated employees. We conducted our fieldwork at vendor corporate offices and at VA medical facilities in Columbia and Kansas City, MO; and San Antonio and Temple, TX from November 2010 through January 2011.

Reliability of Computer-Processed Data

We did not request computer-processed data for this review. We evaluated the sufficiency and accuracy of information provided in connection with the vendor's contracts, workflow processes, and system security controls.

Compliance With CIGIE Standards

We conducted our review in accordance with *Quality Standards for Inspections* published by the Council of the Inspectors General on Integrity and Efficiency. We planned and performed the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objective.

Appendix B Background

Contractor Services

The contractor provides automated communications solutions for healthcare providers and patients. In FY 2011, the vendor's contracts are valued at approximately $5.2 million and include services for 141 VA medical facilities. Since 1992, the vendor has provided the VA with hardware and proprietary software offering veterans telecommunications services to remotely access VistA applications. The contractor's primary services to VA are described below.

Table

Contractor Services Provided to VA

Suite	Description
Pharmacy Suite	Prescription inquiry and refill order processing via telephone Prescription-specific medication information available to patients Prescription renewal requests via telephone
Scheduling Suite	Appointment reminder notifications with patient feedback options via telephone Patient-initiated appointment inquiries and cancellations via telephone Clinic-initiated appointment cancellation notifications Patient-initiated phone number verification and re-entry
Financial Suite	Patient-initiated automated balance inquiries via telephone
Clinical Suite	Preventive health messages/ customized patient surveys Secure physician-patient communications such as lab results via telephone Automated staff emergency notification system via telephone

Automated Access

Patients call a phone number provided by VA medical facilities to access contractor automated services. The contractor's automated system answers these calls with customizable recordings, which provide various patient services. Calls are routed to systems hosted at most VA medical facilities. Contractor systems interconnect with VistA through common network protocol services. To provide nationwide support, personnel connect to VA networks and contractor systems using Virtual Private Network user accounts and remote desktop solutions.

Appendix C Agency Comments

Department of Veterans Affairs

Memorandum

Date: July 1, 2011

From: Principal Deputy Assistant Secretary for Information and Technology (005A)

Subj: Draft OIG Report – Review of Alleged Unauthorized Access to VA Systems

To: Director, Information Technology and Security Audit Division (52CT)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, ***"Review of Alleged Unauthorized Access to VA Systems."*** The Office of Information and Technology concurs with OIG's findings and submits the attached revised written comments to the report.

We appreciate your time and attention to our information security program. If you have any questions, feel free to call me at 202-461-6910, or have a member of your staff contact Ruth Cannatti, Acting Deputy Associate Deputy Assistant Secretary for Cyber Security (005R2), at 202-461-6410.

(original signed by:)

Stephen W. Warren

Attachment

005 Attachment

Office of Information and Technology
Response to draft OIG Report,
"Review of Alleged Unauthorized Access to VA Systems"

RECOMMENDATION 1: We recommend the Assistant Secretary for Information and Technology implement procedures to ensure information security officers and systems administrators actively monitor contractor user accounts for inappropriate use and terminate accounts for separated contractor personnel on a timely basis.

OIT Response: ***Concur***. Contractor user accounts will be monitored for inappropriate use and terminated for separated personnel in accordance with the terms of the vendor contract and the provisions of VA Handbook 6500 (Information Security). This includes a quarterly review by the Contracting Officer Technical Representative (COTR) to assure the need for account continuation.

It should also be noted that the contractor plays a major role in ensuring compliance with VA information security requirements and must adhere to these requirements if VA systems and information are to be adequately protected. The vendor's contract incorporates VA Handbook 6500 which prohibits the sharing of user accounts. In addition, regarding termination of personnel, Section D/Attachment 1of their contract requires that the vendor:

- Deny all terminated personnel physical and electronic access to all data, IT equipment, and systems
- Inform the contractor's program manager and Contracting Officer Technical Representative (COTR) within 24 hours of any employee termination.

When notified by the contractor of the termination of personnel, the COTR will contact the National VA Helpdesk to log a Remedy system ticket with the appropriate VISTA support team requesting that the user account be terminated.

RECOMMENDATION 2: We recommend the Assistant Secretary for Information and Technology evaluate and upgrade risk designation level for contractor personnel to "Moderate," in accordance with VA information security requirements, and ensure commensurate background investigations are performed for those personnel with access to VA systems and sensitive information.

OIT Response: ***Concur.*** The OIT program manager will request that the Contracting Officer (CO) modify the vendor's contract to upgrade the risk designation level for contractor personnel to "Moderate" which requires a Minimum Background Investigation (MBI) for personnel working on the contract.

In accordance with the provisions of VA Handbook 0710 (see below) the COTR will then ascertain whether a prior MBI investigation was completed and is still valid on all contract personnel and:

- If an MBI investigation has been completed and is still valid, contractor personnel will provide certification to the CO/COTR who in turn, provides this information to the Security and Investigations Center (SIC).

- If an MBI investigation has not yet been completed or is no longer valid, the CO/COTR will provide the names of the contractor personnel to the SIC who will then initiate a request to the Office of Personnel Management (OPM) for performance of an MBI. The SIC will then adjudicate the background investigation and the CO/COTR will ensure that it is on record in accordance with VA Directive and Handbook 0710 and take the appropriate action based on the results of the investigation.

RECOMMENDATON 3: We recommend the Assistant Secretary for Information and Technology request that the Deputy Assistant Secretary for Acquisition and Logistics modify the vendor's contract to increase background security requirements for contractor personnel with access to VistA mission critical systems.

OIT Response: ***Concur.*** The OIT program manager will request that the CO upgrade the position sensitivity and background investigation level (contained in Section D, Attachment 1) of the vendor contract to "Moderate." When this requirement has been incorporated into the contract, the COTR will provide the names of contractor personnel who do not have a completed MBI on file to the SIC who will then initiate a request to OPM for performance of an MBI. The SIC will then adjudicate the background investigation and the COTR will ensure that it is on record and take the appropriate action based on the results of the investigation.

RECOMMENDATION 4: We recommend the Assistant Secretary for Information and Technology require contractor personnel to complete initial and, as appropriate, refresher security awareness training and sign the Contractor Rules of Behavior to ensure full awareness of VA information security requirements when accessing VA systems and networks.

OIT Response: ***Concur. Action Completed.*** VA Handbook 6500 and the security provisions of the vendor contract already require that personnel with access to VA information systems and networks (1) complete initial and, as appropriate, refresher security awareness training and (2) sign a Rules of Behavior to ensure full awareness of VA information security requirements. The COTR will ensure that contractor personnel complete all annually required VA security training and retain copies of certificates for such training and National Rules of Behavior and Non-Disclosure forms.

Additionally, to emphasize the need for compliance with VA information security requirements, OIT will send a letter to the vendor, reminding them of their responsibilities for, and the consequences of, failure to comply with these requirements. Target date for issuance of this letter is July 31, 2011.

RECOMMENDATION 5: We recommend the Assistant Secretary for Information and Technology review the contractor's system security controls and practices to ensure compliance with VA's information security requirements.

OIT Response: ***Concur.*** Consistent with the provisions of VA Handbooks 6500 (Information Security) and 6500.3 (*Certification and Accreditation of VA Information Systems*) and the vendor contract (Section D, Attachment 1 Addendum B), the Director of the OIT Certification Program Management Office will contact the COTR for the vendor contract to schedule a review of the contractor's system security controls. OIT will determine from this review if contractor systems meet VA information security requirements and, in conjunction with the CO/COTR, take action, as appropriate. Target date for initiation of these actions is July 31, 2011.

Appendix D 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	Michael Bowman, Director Tom Greenwell Jack Henserling Shawn Hill George Ibarra Ryan Nelson Steve Slawson

Appendix E Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Assistant Secretaries
Office of General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report will be available in the near future on the OIG's Web site at http://www.va.gov/oig/publications/reports-list.asp. This report will remain on the OIG Web site for at least 2 fiscal years.