VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Unauthorized System Interconnection at the VA Regional Office in Wichita, Kansas

April 6, 2017
16-00376-133

ACRONYMS

CIO	Chief Information Officer
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
ISA	Interconnection Security Agreement
ISO	Information Security Officer
KCVA	Kansas Commission on Veterans Affairs
MOU	Memorandum of Understanding
NSOC	Network Security Operations Center
OIG	Office of Inspector General
OI&T	Office of Information and Technology
VA	Department of Veterans Affairs
VARO	VA Regional Office
VPN	Virtual Private Network
VSO	Veterans Service Organization

Highlights: Review of Unauthorized System Interconnection at the VARO in Wichita, KS

Why We Did This Review

The VA Office of Inspector General (OIG) Hotline division received an allegation that an unauthorized system interconnection existed between a Veterans Service Organization (VSO) network and the Wichita, Kansas, VA Regional Office (VARO). More specifically, the allegation stated that a system interconnection existed without a required Interconnection Security Agreement in place to define applicable information security requirements. The complaint also stated that the system interconnection was not disclosed to the OIG during a recent Federal Information Security Modernization Act audit.

What We Found

We substantiated the allegation that an unauthorized system interconnection existed between the Wichita VARO and the Kansas Commission on Veterans Affairs Office network. Specifically, we noted that the system interconnection was established in 2013 without negotiating any VA review processes or change management procedures including a required Interconnection Security Agreement. We also substantiated the allegation that the system interconnection was not disclosed to the OIG because Office of Information Technology (OI&T) staff did not believe the connection constituted a formal system interconnection according to VA policy.

The unauthorized system interconnection occurred because OI&T technical staff did not have the technical knowledge or exercise due diligence to identify the system interconnection in accordance with VA policy, did not follow VA's change management procedures for reviewing and approving significant network and system changes, and Wichita VARO did not have a formal process in place for managing VSO system change requests that may adversely affect VA's network environment.

As a result, the unauthorized system interconnection violated VA policy and the computers used by VSO representatives were inappropriately allowed to use client software to establish simultaneous network connections between VA's and the VSO's networks.

What We Recommended

We recommended the Assistant Secretary for Information Technology, in conjunction with the Wichita VARO facility director, ensure that the network interconnection with the Kansas Commission of Veterans Affairs is brought into compliance with VA information security requirements.

Agency Comments

The Principal Deputy Under Secretary for Benefits and the Acting Assistant Secretary for Office of Information and Technology concurred with our findings and recommendations. We will follow up on the implementation of corrective actions.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

Introduction 1

Results and Recommendations 2

Finding — Controls To Identify and Secure Unauthorized System Interconnections Need Improvement 2

Recommendations 8

Appendix A — Background 10

Appendix B — Scope and Methodology 11

Appendix C — Management's Comments 12

Appendix D — Contact and Staff Acknowledgments 17

Appendix E — Report Distribution 18

INTRODUCTION

Objective

We conducted this review to determine the merits of a Hotline complaint alleging that an unauthorized system interconnection existed between a Veterans Service Organization (VSO) network and the Wichita, KS, VA Regional Office (VARO). Additionally, we evaluated whether system interconnections were disclosed to the Office of Inspector General (OIG) during a recent Federal Information Security Modernization Act (FISMA) audit.

Allegation and Background

The VA OIG Hotline division received an allegation in October 2015 that an unauthorized system interconnection existed between a VSO network and the Wichita, KS, VARO. More specifically, the allegation stated that a system interconnection existed without an Interconnection Security Agreement in place to define information security requirements, as required by VA policy. The complaint also stated that the system interconnection was not disclosed to the OIG during the FY 2015 FISMA audit.

VA is authorized[1] to partner with VSOs to assist veterans who are applying for VA benefits. To facilitate this partnership, VA provides office space to a number of VSOs that are located in buildings owned or occupied by the Department. The Kansas Commission on Veterans Affairs (KCVA) has accredited Veterans Service Representatives located at the Wichita VA Medical Center, Wichita VARO, and the Eastern Kansas Health Care System Topeka and Leavenworth campuses. The KCVA Quality Assurance office at the Wichita VARO receives veterans' claims from each VSO campus and field offices before final processing and delivery to VA.

In 2013, KCVA management requested a direct connection from VA networks to its claims management system to expedite the collection of veterans' claim information. Subsequently, the facility Chief Information Officer (CIO) approved a system interconnection between an external VSO network and the Wichita VARO and the use of Virtual Private Network (VPN) software hosted on computers used by KCVA Veterans Service Representatives.

[1] 38 USC § 5902.

RESULTS AND RECOMMENDATIONS

Finding

Controls To Identify and Secure Unauthorized System Interconnections Need Improvement

We substantiated the allegation that an unauthorized system interconnection existed between the Wichita VARO and the Kansas Commission on Veterans Affairs (KCVA) network. Specifically, we noted that the system interconnection was established in 2013 without negotiating any VA review processes or change management procedures. We also substantiated the allegation that the system interconnection was not disclosed to the OIG because Office of Information and Technology (OI&T) staff did not believe the network connection constituted a formal system interconnection in accordance with VA policy.

The unauthorized system interconnections occurred because OI&T technical staff did not:

- Have the technical knowledge or exercise due diligence to appropriately identify the system interconnection in accordance with VA policy
- Follow VA's change management procedures for reviewing and approving significant network and system changes

Furthermore, the Wichita VARO did not have a process in place for managing VSO system change requests that may adversely affect VA's network environment. As a result, KCVA Veterans Service Representatives were inappropriately allowed to use client software on assigned computers to establish simultaneous network connections between VA's internal network and the VSO network. Consequently, VA's internal networks faced unnecessary risks of unauthorized access and malicious activity from external networks over an extended period of time without detection. In October 2016, VA reported that the unauthorized client software was removed; thus eliminating the concurrent network connection between VA's internal network and the KCVA network. In December 2016, the Principal Deputy Under Secretary for Benefits stated that VA is also working to revise existing policy to differentiate when non-VA employees should contact a designated regional office point of contact versus when they should contact the National Service Desk for assistance in resolving technical issues.

Background and Criteria

VA Handbook 6500 and VA Directive 6004 change management policy and procedures require full review, documentation, and appropriate management signatory authority before enacting any changes to systems and networks. VA requires system owners to use VA Handbook 6500. Appendix F of the Handbook provides the methodology for system owners to use in documenting system support and interconnectivity agreements in accordance

with Federal guidance. According to Appendix F, the Information System Owner must consider the risks that may be introduced when systems are connected and determine the appropriate controls employed.

The National Institute of Standards and Technology Special Publication 800-47 characterize an interconnection as a direct connection of two or more Information Technology systems by either a leased line or VPN for the purpose of sharing informational resources.[2] VA policy requires all system interconnections to have Interconnection Security Agreement (ISA) unless both systems have the same authorizing official.[3] An ISA is used to describe the security controls that will be used to protect the interconnecting systems. Office of Management and Budget Circular A-130 also requires agencies to obtain written management authorization before connecting their systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection.

Allegations Substantiated

We substantiated the allegation that an unauthorized system interconnection existed between the Wichita VARO and the KCVA network. Specifically, in 2013, KCVA management requested a direct connection from VA networks to its external claims management system in order to expedite the collection of veterans' claim information. Despite VA policy to the contrary, the facility CIO approved a system interconnection between a VSO network and the Wichita VARO without negotiating any VA formal review processes or change management procedures. Moreover, this system interconnection did not have a required Interconnection Security Agreement in place that described the security controls that would be used to protect the systems. Without the proper security agreements in place, external partners may not implement appropriate security controls as required by VA information security policies. This system interconnection remained undocumented until it was reported to the VA Network Security and Operations Center in September 2015.

In October 2015, a network CIO communicated to the Region 5 Information System Director, the central area network Information Security Officer (ISO), and the facility CIO that the VPN connection between the KCVA and VA networks was not a system interconnection because the two networks were not physically connected together. However, the Wichita VARO facility ISO asserted that because the VPN connection traverses the internet, it is technically a system interconnection that allows digital communications to be sent and received. Subsequently, Region 5 OI&T staff further investigated the VPN issue and acknowledged that a system interconnection

[2] National Institute of Standards and Technology, Special Publication 800-47, *Security Guide for Interconnecting Information Technology System*, August 2002.
[3] VA Handbook 6500, Appendix F, Control CA-3.

existed between the Wichita VARO and external KCVA networks prior to our site visit in November 2015. OI&T staff later performed a data call and found that similar interconnections existed at two other regional offices. During our November 2015 site visit, we observed VSO representatives accessing their external claims management system from the VA network using VPN client software on their computers. We also observed a VSO representative transferring and saving data from the KCVA network back to computers connected to the VA network. With the exception of copying and pasting selected veteran information, OI&T and KCVA representatives stated that no VA-owned data were transmitted over the VPN connection or hosted externally on KCVA networks.

We also substantiated the allegation the system interconnection was not disclosed to the OIG during our annual FISMA audit because OI&T staff did not believe the network connection constituted a formal system interconnection in accordance with VA policy. During our FISMA site visit conducted in August 2015, the OIG and its contractors were informed by OI&T staff that no interconnections existed at the site. OI&T staff believed that the VPN connection between the KCVA and VA networks was not a system interconnection because the two networks were not physically connected together. We also noted during the FISMA site visit that the Wichita VARO Facility Compliance Report stated that the facility had no system interconnections. As a result of our Hotline site visit in November 2015, Region 5 OI&T staff further investigated the VPN issue and acknowledged that a system interconnection existed between the Wichita VARO and external KCVA networks. However, we noted that the Facility Compliance Report was not updated to reflect the recently identified system interconnection with the KCVA network.

Reasons for Unauthorized System Interconnection

The unauthorized system interconnections occurred because OI&T technical staff did not:

- Have the technical knowledge or exercise due diligence to identify appropriately the system interconnection in accordance with VA policy
- Follow VA's change management procedures for reviewing and approving significant network and system changes

Further, the Wichita VARO did not have a process in place for managing VSO system change requests that may adversely affect VA's network environment.

Lack of Technical knowledge

We determined that VARO management and OI&T technical staff lacked the technical knowledge to accurately identify the connection as a system interconnection. Specifically, OI&T staff did not have a clear understanding of what constitutes a system interconnection at the Wichita VARO. For instance, the facility CIO and network CIO claimed that the term "interconnection" only applied to physical system connections but not to

logical connections. As a result, they did not consider the use of VPN software to connect VSO representatives to an external network to be a system interconnection that required a formal ISA. The National Institute of Standards and Technology Special Publication 800-47 characterizes an interconnection as a direct connection of two or more Information Technology systems by either a leased line or VPN for the purpose of sharing informational resources. Without properly applying knowledge of applicable information security policies, the security to VA's network infrastructure is at risk of unauthorized access or malicious use by not maintaining set information security standards.

Recommendation 1 addresses the actions needed to improve oversight of system interconnections by providing technical training on the identification of external system interconnections and the required change control processes for managing alterations to systems and network connections.

Lack of Due Diligence

OI&T missed several opportunities to identify the system interconnection between KCVA and Wichita VARO networks and implement appropriate security controls after the interconnection became active in 2013. For instance, in August 2014, KCVA submitted a request to the Eastern Kansas Health Care System ISO requesting an install of VPN software on workstations used by VSO representatives at the VA medical facility. Subsequently, the Eastern Kansas Health Care System ISO contacted the Wichita VARO ISO to obtain an understanding of the KCVA system network, information on existing system configurations, and what formal agreements were in place to authorize the VPN software in use at the Wichita VARO. The Wichita VARO ISO confirmed that VPN software was used to connect VSOs to an external KCVA network; however, the ISO was uncertain whether a formal agreement was needed to authorize the system interconnection. Subsequently, the Eastern Kansas Health Care System ISO advised KCVA that an external connection using VPN software was not authorized and any external system connection with the KCVA network would require an ISA with a security waiver.

While continuing to pursue potential VPN access, the Eastern Kansas Health Care System ISO communicated with various Veterans Health Administration and Veterans Benefits Administration program offices to inquire about other VSO representatives that may be connecting to external networks at other VA facilities. In response, one OI&T staff member stated that VPN software should not be used for external connections from inside VA's network in accordance with VA policy. Despite the various communications stating that the use of VPN software was not authorized, the Wichita VARO ISO did not question whether a system interconnection existed or whether a formal ISA was needed to authorize the connection between the Wichita VARO and KCVA network. The ISO's lack of technical knowledge regarding the identification of a system interconnection was a contributing factor for not taking immediate action to correct the

security violation. According to VA Handbook 6500, responsible ISOs must ensure an appropriate operational security posture is maintained by effectively monitoring changes to the system control environment. Consequently, the Wichita VARO ISO should have evaluated the security effect of the system interconnection and determined whether corrective actions were necessary to ensure compliance with VA information security policies.

In September 2015, OI&T's lack of due diligence was also demonstrated when the Wichita VARO ISO submitted a security ticket to VA's Network Security Operations Center (NSOC) to report an unauthorized system interconnection without a corresponding ISA. Contrary to VA policy, the security ticket was subsequently closed by the NSOC stating that ISAs are to be reviewed and approved by the network system owner, contracting officer representative, and the ISO. According to VA Directive 6513, the VA NSOC is responsible for the monitoring of all external connections for compliance with existing Federal laws and VA policies. Given the NSOC's lack of attention in this area, the Wichita VARO ISO did not understand the purpose of reporting unauthorized system interconnections to the center.

Based on our review, OI&T staff had ample opportunities to identify the unauthorized Wichita VARO system interconnection for remediation. Despite ongoing communication stating that the use of VPN software was unauthorized, VA staff failed to investigate the interconnection further, properly apply knowledge to identify the system interconnection, or take any appropriate action to properly secure VA's network. Without appropriate training and accountability for compliance with VA information security policies, VA staff will not be adequately prepared to ensure the proper security of VA's network infrastructure.

Recommendation 2 addresses the need to implement review processes to monitor the performance of the facility CIOs, ISOs, and technical staff on the identification of external system interconnections and the required change control processes.

Recommendation 3 addresses the need to formalize an Interconnection Security Agreement and ensure the existing interconnections meet VA security requirements.

Change Management Procedures Not Followed

Contrary to established VA policy, in 2013, the facility CIO approved a system interconnection between a VSO network and the Wichita VARO without following any VA formal review process or change management procedures. More specifically, the facility CIO approved the use of VPN software on computers used by VSO representatives without first investigating whether it was appropriate to authorize the use of such software to connect to the KCVA external network. Consequently, the facility CIO approved a prohibited outbound connection with external network resources.

VA Handbook 6500 and VA Directive 6004 change management policy require a full review, documentation, and appropriate management signatory authority before enacting any significant network or system changes. In addition, the VPN software was not approved for use by the Network Security Operations Center, Enterprise Systems Engineering, and the local ISO, as required by VA policy. Moreover, the VPN connection to an external network was not approved by the Enterprise Security Change Control Board in accordance with VA Directive 6004. Because the facility CIO acted independently when approving the system interconnection, the network system owner was denied the opportunity to evaluate the proposed system connection, determine the risks associated with the interconnection and concurrent VPN connections, or require the implementation of certain controls to ensure VA information security standards were maintained.

Recommendation 4 addresses the need for VA to conduct annual reviews of all VSO systems connected to VA's network to ensure that appropriate security controls are in place.

Recommendation 5 addresses the actions needed to implement improved change management controls to help prevent concurrent VPN connections at VA regional offices.

No Formal Process for Managing VSO Service Requests

We determined that the Wichita VARO lacked a formal process for managing VSO change requests, which contributed to the noncompliance with set policy when approving a system interconnection between Wichita VARO and the KCVA network. In addition, the Wichita VARO staff could not provide a formal Memorandum of Understanding or Business Partner Agreement that defines roles and responsibilities of key stakeholders and their partnership with the Wichita VARO when managing VSO service requests. National Institute of Standards and Technology Special Publication 800-47 recommends the use of a formal agreement with any external partner that shares agency resources to manage the terms, conditions, responsibilities, and authorities of the participating organizations. Without a formal change management process in place, VSO representatives were forced to rely on the judgment of the local facility CIO when authorizing the interconnection between Wichita VARO and the KCVA network. Additionally, a change management process is needed so the Wichita VARO will have consistent processes in place for handling VSO service requests while complying with VA policy requirements. Implementing a formal change management process would also help ensure that all VSO service requests are reviewed by appropriate stakeholders in accordance with VA policy.

Recommendation 6 addresses the actions needed for the Wichita VARO to implement a local change management process to handle service requests from local VSOs.

Effects of Unknown System Interconnections

We determined that the system interconnection between Wichita VARO and KCVA poses significant risk to VA's network because it fails to meet VA information security standards. Specifically, we verified that the system interconnection created a network bridge, which allows the exchange of data between the internal VA network and the external KCVA network. Additionally, we noted that the network bridge allows VSO users to be on both networks simultaneously through the use of a VPN split tunnel. Consequently, if KCVA's network is infected with hostile software such as viruses, spyware, or a Trojan horse, VSO users could become conduits for spreading malware to the rest of the VA network through the VPN connection. Moreover, the use of VPN split tunneling enables VSO users to bypass VA gateway-level security monitoring and is therefore considered a prohibited practice according to VA Information Security policy and VA Handbook 6500. Every VPN connection from VSO representatives creates a unique instance of this security weakness. During our November 2015 review, we were informed that nine VSO employees were connecting to the KCVA network via the VPN application, thus creating nine separate network bridges.

Conclusion

VSOs provide a significant service and invaluable support to VA in completing its mission of providing benefits and services to veterans. However, effective information security controls and oversight between organizations sharing access to information are paramount to protecting VA's network from unauthorized access and malicious activity. VA has clear policies that require all system changes be monitored through a change management process. This control was circumvented when VSO representatives were allowed to connect to external networks without proper VA approval or coordination. For every system interconnection, it is essential for an ISA to be executed and enforced to ensure that appropriate security controls are in place on external systems connecting to VA networks. Our review noted that the system interconnection between VA and the KCVA violates Department policy and places VA's network at risk of unauthorized access and malicious behavior.

Recommendations

1. We recommended the Assistant Secretary for Information and Technology mandate refresher training for facility chief information officers, information security officers, and technical staff on the identification of external system interconnections and the required change control processes for managing alterations to systems and network connections.

2. We recommended the Assistant Secretary for Information and Technology implement review processes to monitor the performance of the facility chief information officers, information security officers, and

technical staff on the identification of external system interconnections and the required change control processes.

3. We recommended the Assistant Secretary for Information and Technology, in conjunction with the Wichita VA Regional Office Director, ensure that VA's system interconnection with the Kansas Commission on Veterans Affairs Office is brought into compliance with VA Information Security requirements and is authorized by an Interconnection Security Agreement and Facility Compliance Report.

4. We recommended the Assistant Secretary for Information and Technology conduct an annual review of all Veterans Service Organization systems connected to VA's network and ensure that appropriate Interconnection Service Agreements are in place and enforced for those connections.

5. We recommended the Assistant Secretary for Information Technology implement improved change management controls to prevent the establishment of Virtual Private Network concurrent network connections that are not in accordance with VA policy.

6. We recommended the Director of the Wichita VA Regional Office implement a local process for managing all Veterans Service Organization service requests and document pertinent roles and responsibilities within a Memorandum of Understanding.

Management Comments and OIG Response

The Principal Deputy Under Secretary for Benefits and the Acting Assistant Secretary for Office of Information and Technology concurred with our findings and recommendations and have requested closure of certain report recommendations. Based on the information provided, we consider recommendations 1, 3, and 5 closed at this time. For recommendation 6, we request that the Principal Deputy Under Secretary for Benefits provide a corrective action plan to demonstrate the Wichita VA Regional Office has implemented a local process for managing all VSO service requests.

We will monitor the Wichita VA Regional Office and the Office of Information and Technology's implementation of corrective actions until all proposed actions are completed. Appendixes C and D contain the full text of the comments of the Principal Deputy Under Secretary for Benefits and the Acting Assistant Secretary for Office of Information and Technology.

Appendix A Background

VSO Authority

In accordance with Title 38 USC § 5902, VA may recognize organizations specifically for assisting claimants for VA benefits in the preparation, presentation, and prosecution of their disability claims. 38 CFR § 14.628 prescribes the application requirements for recognition of national, state, and regional or local organizations.

The regulations further authorize the VA Secretary to furnish office space in buildings owned or occupied by VA, for the use of recognized representatives of national organizations and accredited State organizations. In the case of a facility under the control of the Veterans Benefits Administration or the Veterans Health Administration, the final decision on such matters will be made by the Under Secretary for Benefits or the Under Secretary for Health, respectively.[4] Finally, accredited service organization representatives, claims agents, and attorneys may obtain read-only remote access to the electronic VA claims records for the claimants they represent.

KCVA VSO

The Kansas Commission of Veterans Affairs Office is a State VSO that uses office space at the Wichita VARO. VA has allowed KCVA to share its network giving VSO representatives direct network access to applications hosted within the VA network. KCVA also has a presence at the Topeka and Leavenworth VA medical facilities. In addition to requirements for accreditation under the law, the VSO must meet all security requirements mandated by VA policy. VSO access to VA's claims records is read-only for the claimants they represent. Accredited VSO representatives may securely connect to available remote VBA applications using their own internet service provider.

[4] 38 USC § 5902

Appendix B Scope and Methodology

Scope

We conducted our review from November 2015 through November 2016. Our assessment of internal controls focused on those processes relating to our review objectives. Our review evaluated the merits of a VA Hotline allegation that an unauthorized network system interconnection existed with a VSO network at the Wichita VARO. We also evaluated why VA did not report the interconnection during our FY 2015 FISMA audit and whether the appropriate security agreements and controls were in place to enforce applicable information security requirements. Finally, we evaluated the security risks that can expose VA's network to unauthorized access and malicious activity.

Methodology

To accomplish this review, we obtained and reviewed relevant documentation. Our review focused only on co-located VSO representatives with direct network access from their computers to VA's internal network. We interviewed the Wichita VARO Director, KCVA officials, and OI&T technical staff to evaluate the history and oversight of the alleged system interconnection. Additionally, we collected evidence that revealed the exact configuration of the computer connection to the external network. We researched applicable VA directives, handbooks, Federal information security requirements, and identified relevant business practices and information security controls. We evaluated the VPN software configuration settings and network traffic to verify the existence of the VPN split tunnel capability. We also assessed VA's monitoring procedures for identifying and overseeing system interconnections. We did not identify any malicious activity associated with the unauthorized system interconnection.

Data Reliability

We did not request computer-processed data for this review. We evaluated the sufficiency and accuracy of information provided in connection with personal testimony, staff email correspondence, and direct observation.

Government Standards

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* The evidence obtained provides a reasonable basis for our findings and conclusions based on our review objective.

Appendix C Managements Comments – Office of the Secretary for Benefits

Department of Veterans Affairs Memorandum

Date: December 27, 2016

From: Office of the Under Secretary for Benefits (20)

Subj: OIG Draft Report—Review of Unauthorized System Interconnection at the Wichita VA Regional Office [Project No. 2016-00376-CT-0020]—VAIQ 7761463

To: Assistant Inspector General for Audits and Evaluations (52)

1. Attached is VBA's response to the OIG draft report: Review of Unauthorized System Interconnection at the Wichita VA Regional Office.

2. Questions may be referred to Ruma Mitchum, Program Analyst, at 632-8987.

(original signed by:)

Thomas J. Murphy
Principal Deputy Under Secretary for Benefits Performing the Duties of Under Secretary for Benefits

Attachments

Attachment

Veterans Benefits Administration (VBA)
Comments on OIG Draft Report
Review of Unauthorized System Interconnection at the Wichita VA Regional Office

VBA concurs with OIG's findings in the draft report and provides the following comments in response to the recommendations:

Recommendation 3: We recommended the Assistant Secretary for Information and Technology, in conjunction with the Wichita VA Regional Office Director, ensure that VA's system interconnection with the Kansas Commission on Veterans Affairs is brought into compliance with VA information security requirements and is authorized by an Interconnection Security Agreement and Facility Compliance Report.

VBA Response: VBA defers to the Office of Information and Technology.

Recommendation 6: We recommended the Director of the Wichita VA Regional Office implement a local process for managing all Veteran Service Organization service requests and document pertinent roles and responsibilities within a Memorandum of Understanding.

VBA Response: Concur. VBA recently released VBA Letter 20-16-08, Internal VBA Systems Access for Claimant and Appellant Representatives (attached), describing the processes through which representatives may request and receive access to the VA network and VBA claims processing systems. VBA is further working to revise VBA Letter 20-16-08 to differentiate when a non-VA employee should contact a designated regional office point of contact versus when they should contact the National Service Desk for assistance in resolving technical issues within the scope of the non-VA employee's approved access capabilities.

VBA requests closure of this recommendation.

For accessibility, the format of the original documents in this appendix has been modified to fit in this document

Appendix D Managements Comments – Office of the Assistant Secretary for Information and Technology

Department of Veterans Affairs Memorandum

Date: February 23, 2017

From: Acting Assistant Secretary for Information and Technology (005)

Subj: OIG Draft Report, "*Review of Unauthorized System Interconnection at the Wichita VA Regional Office*"

To: Assistant Inspector General for Audits and Evaluations (52)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, "Review of Unauthorized System Interconnection at the Wichita VA Regional Office". The Office of Information and Technology concurs with OIG's findings and submits the attached written comments for recommendations 1 thru 5.

If you have any questions, contact me at (202) 461-6910 or have a member of your staff contact Dominic Cussatt, Acting Deputy Chief Information Officer for Information Security at (202) 461-0044.

(original signed by:)

ROB C. THOMAS, II

Attachments

Attachment

Office of Information and Technology (OI&T)
Comments on OIG Draft Report:
"Review of Unauthorized System Interconnection at the Wichita VA Regional Office"

OIG Recommendation 1: We recommended the Assistant Secretary for Information and Technology mandate refresher training for facility Chief Information Officers, Information Security Officers, and technical staff on the identification of external system interconnections and the required change control processes for managing alterations to systems and network connections.

OIT Comments: Concur. VA OIT through the Office of Information Security (OIS) Field Security Service provides annual memorandum of understanding (MOU) and interconnection security agreement (ISA) training through the Continuous Readiness in Information Security Program (CRISP) FOCUS campaign effort. The training is available to all OIT staff. The training includes FSS guidance to the field on the document process steps including identification and documenting changes. The training for FY16 was conducted in December 2015. The training for FY17 is scheduled for December 14 and December 16, 2016. We request closure of this recommendation based on the evidence provided above.

Complete December 2016.

OIG Recommendation 2: We recommended the Assistant Secretary for Information and Technology implement review processes to monitor the performance of the facility Chief Information Officers, Information Security Officers, and technical staff on the identification of external system interconnections and the required change control processes.

OIT Comments: Concur. VA OIT though OIS /FSS has an annual action Item in place to review and update ISA/MOU. The review and update is a collaborative process with the ISO and CIO to ensure proper documentation of connections and identification deficiencies. In FY16 IT Operations (formerly Service Delivery and Engineering) conducted a physical inventory of all external network connections. The action item for FY 17 was released January 18 with a completion date of March 31, 2017. The Network Security Operations Center (NSOC) maintains a list of authorized external connections. That list is monitored. To monitor the performance of the CIO, ISO, and support staff in meeting ISA/MOU requirement OIS recommends the OIT Office of Quality, Privacy, and Risk (QPR) establish a process to review the OIT ISA/MOU process including the effectiveness of the annual action item.

Ongoing – Completion Due Date March 31, 2017.

OIG Recommendation 3: We recommended the Assistant Secretary for Information and Technology, in conjunction with the Wichita VA Regional Office Director, ensure that VA's system interconnection with the Kansas Commission on Veterans Affairs is brought into compliance with VA information security requirements and is authorized by an Interconnection Security Agreement and Facility Compliance Report.

OIT Comments: Concur. On August 16, 2016 a MOU-ISA was signed for the Wichita RO and the KCVA. OI&T entered Enterprise Security Change Control Board (ESCCB) request 10A03771 on August 30, 2016 for approval to configure a Site-to-Site (S2S) VPN connection between VA and KCVA. The ESCCB request was approved by the ESCCB Chair on September 21, 2016, connection ID 0104. National Service Desk ticket R10759003FY16 was opened to configure and test the approved connection. In conjunction with the configuration and successful testing of the S2S VPN connection, the CISCO AnyConnect software was removed from all KCVA workstations and was verified as completed by the ISO and FCIO on October 6, 2016. The KCVA individuals were migrated to use the S2S connection successfully, and they are able to perform their duties without issue. The Interconnection Security Agreement and Memorandum of Understanding have been uploaded to the RiskVision Governance, Risk, and Compliance (GRC) tool and is captured in the Wichita Regional Office Facility Compliance Report.

We request closure of this recommendation based on the evidence provided above. Complete December 2016.

OIG Recommendation 4: We recommended the Assistant Secretary for Information and Technology conduct an annual review of all Veteran Service Organization systems connected to VA's network and ensure that appropriate Interconnection Service Agreements are in place and enforced for those connections.

OIT Comments: Concur. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Programs requires Interconnection Service Agreements (ISA) and Memorandums of Understanding (MOU) (ISA/MOUs) to be reviewed on an annual basis. VA OI&T is conducting annual reviews of all interconnected Veteran Service Organizations with ISA/MOUs in place annually. OI&T Field Security Service (FSS) also conduct Action Items annually to collect and require the local Information Security Officers (ISOs) to review all ISA/MOUs in their prevue. This entails, full review of the ISA/MOU and verification that the connection is still in place, still required, and that no significant changes to the ISA/MOU or the connection have occurred. Sign off certification for completion of the verification review is also documented. In the event of significant changes to the interconnection at any time or if major changes were needed, the agreement must be updated, re-approved and re-signed. We request closure of this recommendation based on the evidence provided above.

Complete December 2016.

OIG Recommendation 5: We recommended the Assistant Secretary for Information Technology implement improved change management controls to prevent the establishment of Virtual Private Network concurrent network connections that are not in accordance with VA policy.

OIT Comments: Concur. OIT has an existing change control process in place. To improve security measures, the Technical Reference Manual (TRM) has added the following requirement for the AnyConnect Secure Mobility Client (June 15, 2016): In cases where the technology is used for external connections, a full Enterprise Security Change Control Board (ESCCB) review is required in accordance with VA Directive 6004, VA Directive 6517, and VA Directive 6513. The local ISO can advise on the ESCCB review process. The VA Enterprise Security Change Control Board (ESCCB) was established to provide a board charged with the responsibility for ensuring all proposed changes to VA are reviewed to ensure that they are viable and will not adversely impact the operation of the existing system or subsystem. We request closure of this recommendation based on the evidence provided above. Complete December 2016.

All changes to the VA's network infrastructure must be submitted to the ESCCB for evaluation and approval.

OIG Recommendation 6: We recommended the Director of the Wichita VA Regional Office implement a local process for managing all Veteran Service Organization service requests and document pertinent roles and responsibilities within a Memorandum of Understanding.

OIT Comments: Concur.

Please confirm status with Wichita VA Regional Office.

For accessibility, the format of the original documents in this appendix has been modified to fit in this document

Appendix E OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman Carol Buzolich Jerry Charles Juan Rivera Felita Traynham

Appendix F Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans Appeals

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
U.S. Senate: Jerry Moran, Pat Roberts
U.S. House of Representatives: Lynn Jenkins, Roger Marshall, Kevin Yoder

This report is available on our website at www.va.gov/oig.