SECURITY WEAKNESSES IN DOT'S COMMON OPERATING ENVIRONMENT EXPOSE ITS SYSTEMS AND DATA TO COMPROMISE

Department of Transportation

Report No. FI-2013-123
Date Issued: September 10, 2013

This document contains information exempt from mandatory disclosure under FOIA. Exemptions 3 and 7(e) apply.

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Security Weaknesses in DOT's Common Operating Environment Expose Its Systems and Data to Compromise
Report No. FI-2013-123

Date: September 10, 2013

From: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Chief Information Officer

In 2003, the Department of Transportation (DOT) implemented a common operating environment (COE) network to centralize its information technology (IT) services. The Office of the Chief Information Officer (OCIO) manages the COE, which provides email management, computer infrastructure, internet access, and other IT services to over 10,000 users in all of DOT's operating administrations (OA) except the Federal Aviation Administration. Due to the COE's centralized nature, any security vulnerabilities within the COE put its users at risk for compromise, and could impair DOT's ability to accomplish its mission.

We initiated this audit to review DOT's security controls for protecting the COE and the information it contains. Our objectives were to determine: (1) whether the COE is as safe from compromise as possible; and (2) what, if any, security vulnerabilities the COE contains.

To conduct our work, we reviewed the COE's network documentation and security policies to establish a baseline view of the environment. We performed external and internal assessments that covered the COE's entire network. These assessments included penetration tests,[1] vulnerability scans, and manual tests of networked systems, websites, and infrastructure to identify any weaknesses in DOT's security controls. We also interviewed COE personnel. As part of this audit we selected a statistical sample of 134 of 5,735 computers that allowed us to

[1] Penetration testing validates or invalidates security controls' proper operation by emulating methods hackers use to compromise systems.

FOR OFFICIAL USE INFORMATION WAS REDACTED FOR PUBLIC RELEASE

project the number of computers that had critical vulnerabilities.[2] Exhibit A provides more details on our scope and methodology. We conducted our audit work from February 2012 to July 2013 in accordance with generally accepted Government auditing standards.

RESULTS IN BRIEF

~~(FOUO)~~ The COE is not secure from compromise. During our penetration testing—tests that are similar or identical to attacks by hackers—we gained full access to the COE network. The National Institute of Standards and Technology (NIST) provides comprehensive guidance to agencies on how to protect their networks from intrusions. NIST also provides guidance on handling security incidents, including intrusions such as the unlimited access we gained to the network. But the COE's incident handling process did not detect our intrusion. As a result, we continued to have full access for over a week before the COE's management discovered and terminated our presence on the network. [redacted] These deficiencies, which are the result of ineffective security controls, put the COE at risk of unauthorized access and its systems and information at risk of compromise.

(~~FOUO~~) The COE contains vulnerabilities that could allow the compromise of sensitive data. Thirty of 205 servers with internet accessible websites contained critical vulnerabilities. [redacted] Furthermore, OCIO does not maintain an accurate inventory of computer devices on the COE, preventing the identification of unauthorized systems. The COE also has weak user identity authentication controls because OCIO has not fully implemented multifactor identity authentication,[3] and [redacted] Finally, OCIO does not perform required security testing on the COE to identify and remediate common vulnerabilities typically used by network attackers, and does not effectively document vulnerabilities for resource allocation and remediation.

[2] A critical vulnerability requires immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems.

[3] Multifactor authentication requires users to provide at least two methods of identity authentication, such as a password and a personal identity verification card, security token, or biometric, such as a fingerprint, to access the information system.

[4] A password, such as the word "password," is weak if it is relatively easy to guess.

NIST, the Office of Management and Budget (OMB), and DOT policies identify requirements to secure networks and reduce these vulnerabilities. The lack of these required controls on the COE puts its networks, systems and data at risk for compromise.

We are making six new recommendations to assist OCIO in securing the COE's sensitive data and critical functions. The recommendations in this report are in addition to four open recommendations from our Federal Information Security Management Act (FISMA) audits, which are identified in Exhibit B.

BACKGROUND

DOT's COE provides ten OAs at the Department's Headquarters in Washington, DC, with IT services, such as data storage, email and web application access, and database services. The COE also provides a centralized environment for applications that OAs use in support of their operations. To use the COE, OAs enter into agreements with OCIO that define their responsibilities, including regular scanning for vulnerabilities, to maintain their applications and systems in a secure manner. Due to its importance to the DOT's mission, OCIO assigned the COE an impact rating of high as defined by NIST.[5]

OMB and NIST provide policies and guidelines to Federal agencies in IT security. DOT's Cybersecurity Compendium establishes policies, processes, procedures, and standards for the Department's information systems security. It also requires OAs to record detected weaknesses in their information systems and plans of action and milestones (POA&M) to correct them in the Department's Cyber Security Assessment and Management (CSAM) system. CSAM tracks system weaknesses and their remediation.

[redacted]

[5] NIST's Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines impact as high if the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic effect on organizational operations, assets, or individuals.

THE COE IS NOT SECURE FROM COMPROMISE

Our penetration testing demonstrated that the COE is not secure from compromise. We were able to gain unauthorized access to the network due to use of insecure user identity authentication methods. COE administrators remained unaware of our access for over a week because an effective method of incident detection for the COE does not exist. Furthermore, OCIO does not ensure that OAs conduct testing of COE users' security awareness and some users were unable to recognize the types of social engineering emails that we sent—types of email frequently used to gain unauthorized access to networks.

We Gained Unauthorized Access to the COE

(~~FOUO~~) Using common computer hacking procedures, we gained unauthorized access to the COE's network and sensitive applications. NIST and DOT policies call for agencies to require a high level of password complexity for system access, such as a minimum number of characters that include a mix of upper and lower case letters, numbers, and special characters. Furthermore, DOT policy requires OAs to employ encryption to prevent unauthorized disclosure of information during transmission. [redacted] These practices made it easy for us to discover and decode network [redacted] using tools and methods available on the internet. By using an administrator's captured user id and password, we gained access to sensitive data such as drug testing results, and legal information. We also gained control of an uninterrupted power supply that the Federal Highway Administration uses to provide backup electrical power to its server. In addition, after accessing the COE network, we were able to intercept and redirect network traffic and gain full access to the Department's other servers and sensitive data.

OCIO's Ineffective Incident Detection Makes the COE Vulnerable

(~~FOUO~~) OCIO cannot always detect and recognize security breaches in the COE. NIST recommends that agencies use automated incident detection methods[6] for high impact systems such as the COE. [redacted] As a result, OCIO did not detect our presence in the COE for over

[6] Software that monitors network security incidents, such as denial of service attacks, unauthorized access and devices that attempt connection to the network.

a week. In addition, once we gained access, we created our own administrative account that OCIO personnel did not detect and remained unaware of until we informed them several weeks later. When we notified them of our successful penetration, COE personnel informed us that the COE's monitoring system did not detect our unauthorized activity. In addition, we performed vulnerability and penetration testing of DOT websites and server security from outside the COE's network that COE administrators also did not detect.

The absence of network surveillance and monitoring allowed our unauthorized interception and manipulation of data transmitted across the network. While OST has a memorandum of agreement with the DOT's Cyber Security Management Center (CSMC)[7] regarding network monitoring and surveillance services for the COE, it does not require its full enforcement. For example, CSMC has not developed a network diagram or collected device configuration data for all active COE network hardware—needed information for proper configuration of tools for scanning and incident detection. OAs must provide CSMC an inventory of all networks and devices in use by their organization. OCIO was unable to provide evidence that it had given this information to CSMC.

The COE Is Vulnerable to Unauthorized Access Due to Users' Nonadherence to Sound Email Security Practices

The COE is also vulnerable to social engineering emails—deceptive emails that are meant to cause people to break security procedures and provide proprietary information such as passwords and account numbers. DOT policy requires OAs to conduct periodic exercises—such as sending emails that contain suspicious links and placing telephone calls asking for sensitive information—to verify that personnel are applying the knowledge learned in required annual security awareness training. In addition, OCIO requires users that access the COE accept the DOT Rules of Behaviors (RoB), which reference the security awareness requirements, prior to accessing the network. OCIO could not provide evidence that it or the OAs conduct periodic exercises to assess the effectiveness of the annual security awareness training and compliance with RoBs related to social engineering e-mails.

To test users' security awareness, we sent emails that were crafted to look suspicious to 493 selected COE users from across the OAs. We found that at least 13[8] users opened the emails, clicked on the links, and were redirected to our test

[7] Established in 2004, DOT's CSMC is responsible for providing intrusion detection monitoring services.
[8] Our testing tool, which did not properly log and process all connections, logged thirteen attempts to connect, but our observation of network traffic showed more connections.

server without their knowledge. Had this been an actual attack, the user would have allowed the attacker access to his or her computer and the COE network. In addition, none of the 493 users reported the suspicious emails to security officials, as DOT's security training suggest.

OCIO'S MANAGEMENT PRACTICES CREATE WEAKNESSES THAT MAKE THE COE VULNERABLE TO COMPROMISE

Some of OCIO's management practices for the COE create security weaknesses that make the system and its data vulnerable to complete compromise. These practices include: poor configuration management and insufficient applications and systems' security testing; lack of an accurate inventory of devices that are connected to the COE; weak user identity authentication methods; a lack of sufficient tracking of system security weaknesses; and a lack of required penetration testing.

OCIO Has Not Securely Configured All COE Systems

OCIO has not properly configured all COE systems to operate securely. NIST recommends security practices for designing, implementing, and operating publicly accessible Web servers, including related network infrastructure issues. In addition, DOT policy requires OAs to allow only the authorized access necessary for users to accomplish their assigned tasks, and to configure information systems to provide only essential capabilities.

We tested 205 public Websites and found that 30 of them had vulnerabilities that could be used to access proprietary data, redirect visitors to malicious sites, take control of server operations, and/or allow unauthorized access to video conferencing. For example:

- (~~FOUO~~) A file server had settings that would allow users to read and write data without passwords and, consequently, easily manipulate data without authority. [redacted]
- (~~FOUO~~) Five servers [redacted] could allow access to all systems running on each server.

[redacted]

- [redacted]

These vulnerabilities increase the risk that the data and personal information of DOT employees, DOT contractors, and the public could be compromised by unauthorized access.

OCIO Lacks an Effective Method to Identify Devices on the COE

OCIO has not implemented a tool to manage the complete inventory of devices connected to the COE's network, including those used for wireless access. DOT's Cybersecurity policy requires all OAs to collect device inventories through scanning and other continuous monitoring efforts. OCIO provided us with output from several inventory tools, but none presented an accurate accounting of the devices present on the network during our tests. For example, OCIO provided documentation generated by Microsoft Sharepoint, which is used to store and track electronic documents or images, and BMC Remedy, commercial software for managing information system assets. However, this documentation did not include a complete list of all devices on the COE.

Furthermore, OCIO cannot identify unauthorized or insecure wireless access points that allow wireless devices, such as cell phones, to connect to a network. It could not account for 443 wireless access points at DOT Headquarters, 190 of which were not secure. For example, 186 access points were not encrypted and 4 used weak encryption. Because it lacks an accurate inventory, OCIO does not know when unauthorized devices are present on the COE's network. As a result, during our review, we were unable to determine which devices were authorized and which were not.

OCIO Has Not Established Multifactor Identity Authentication for COE Users

(~~FOUO~~) OCIO has not implemented multifactor identity authentication for all COE users, [redacted] We first reported this finding in our 2009 FISMA audit.[10] NIST guidance and DOT policy require both employees and contractors to use personal identity verification (PIV) cards for identity authentication. DOT policy also requires system owners and administrators to use

[10] *Audit of DOT's Information Security Program and Practices*, OIG Report FI-2010-023, November 18, 2009.

multifactor authentication to access the accounts that they use to modify systems. OCIO's plans for multifactor authentication include use of PIV cards, but OCIO has not completed implementation of these cards for all Department employees and contractors. [redacted] Because it has not fully implemented multifactor authentication, OCIO cannot be sure that only authorized users can access the COE.

OCIO Does Not Perform Required Security Testing on the COE

OCIO does not ensure that all computer servers connected to the COE are scanned for vulnerabilities or that identified weaknesses are remediated.[11] We selected a random sample of 134 out of 5,735 computers, and were able to scan 99, or 73.9 percent, successfully. We therefore estimate that the number of computers in the universe that could have been scanned successfully at the time of our testing was 4,237.[12] We found 34 (34.3%) out of our 99 computers had 86 Critical Issues. Based on these findings, we estimate that our universe of 4,237 computers had 3,681 critical issues.[13]

(~~FOUO~~) Furthermore, OCIO has not performed penetration testing on security controls to identify and mitigate security weaknesses that could allow the COE's compromise. DOT Cybersecurity policy requires OAs to scan their systems on a monthly basis for vulnerabilities, and to determine when new vulnerabilities were identified and reported. The policy also requires OAs to perform annual penetration testing on high impact systems such as the COE. However, OCIO could not provide us with reports of monthly vulnerability scans for its systems or its OAs' systems. OCIO also could not provide us with evidence that it had performed annual penetration testing on the COE [redacted]

OCIO Does Not Properly Track the COE's Known Weaknesses for Remediation

(~~FOUO~~) OCIO and the OAs do not create, review, and enter POA&Ms into the Department's CSAM system. DOT's Cybersecurity policy requires OAs to enter and maintain all identified security weaknesses and their POA&Ms in CSAM. We

[11] In some cases, OAs have agreed to perform scanning and remediation, but OCIO cannot ensure that this is happening.
[12] Our best estimate of 4,237 computers has a precision of +/-355 at the 90 percent confidence level.
[13] Our best estimate of 3,681 critical issues as a precision of +/-1,100 at the 90 percent confidence level.

could not locate in CSAM the POA&Ms prepared as a result of OCIO's 2012 security certification and authorization assessment[14] [redacted] COE staff told us that they kept identified security weaknesses in a Microsoft access database independent of CSAM. However, this database did not include all required information for effective vulnerability and remediation tracking. Furthermore, the use of any repository other than CSAM hinders the Department's ability to identify, assess, prioritize, and monitor corrective actions for remediating security weaknesses. During our audit, COE staff informed us that they had initiated corrective actions to load security weaknesses into CSAM but did not provide a scheduled date for completion.

CONCLUSION

Cyber threats such as hackers and social engineering present substantial risks to the security of Federal information systems. OCIO and most OAs depend on the COE for vital information technology services, and to protect their sensitive information. However, because of OCIO's weak security management practices, a number of vulnerabilities exist in the COE that could compromise its operations. This lack of important security controls prevents OCIO from fully safeguarding the confidentiality of the sensitive data that resides on the COE, as well as ensuring the availability of COE services, and maintaining the integrity of its information. Until steps are taken to enhance the COE's security controls, outside attackers using the basic methods we used in our tests could seriously compromise the DOT's operations.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. [redacted] Enforce password complexity requirements [redacted] in accordance with Departmental Cybersecurity Compendium Order 1351.37.

2. Monitor OAs periodic exercises that test COE users' knowledge of security requirements when accessing emails on the Government network.

3. Use automated tools, such as vulnerability scanners or Web application scanners to monitor applications residing in the COE on a constant basis, and

[14] OMB Circular A-130, Appendix III states that Federal agencies must certify and accredit their systems for security compliance. Certification and accreditation require each agency to assess its systems for security risks, test security controls, and create POA&Ms to resolve identified weaknesses.

require each OA to mitigate vulnerabilities in its system or remove the systems from the network.

4. Develop and maintain a complete inventory (current registry) of authorized network devices (including wireless) accessible to staff who monitor departmental networks.

5. Ensure the system owners perform regular vulnerability assessments and scans of all internal systems to identify known vulnerabilities and common misconfigurations, and establish a practice to ensure that OAs and OCIO are collaborating and agreeing on remediation plans.

6. Perform annual penetration testing of the COE as required by DOT policy.

AGENCY COMMENTS AND OIG RESPONSE

We provided the Department's OCIO with a draft of this report on July 16, 2013, and received its written response on August 16, 2013, which is included in its entirety as an Appendix to this report. In its response, OCIO concurred with all 6 recommendations. The OCIO reported that the recommendations will receive the highest priority and commits to work with the operating administrations to achieve the results within the planned timeframes.

ACTIONS REQUIRED

We consider OCIO's planned actions and target dates responsive to all our recommendations and consider them resolved but open pending completion of the planned actions. We appreciate the courtesies and cooperation of the Department of Transportation's representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407.

#

cc: Deputy Secretary
Assistant Secretary for Budget and Programs/Chief Financial Officer
CIO Council Members
DOT Audit Liaison, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

We performed our network security assessment between February 2012 and July 2013 at DOT Headquarters in Washington, D.C., and in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To address our audit objectives, we used the guidance provided in NIST SP 800-115 Technical Guide to Information Security Testing and Assessment (September 2008)[15] to perform a penetration test and vulnerability assessment of the COE using widely available tools and techniques. We interviewed DOT's CIO, information technology contractors, and senior leadership to determine what information and resources were critical to COE's operation and how protections were implemented. We reviewed and analyzed documents, policies, and procedures related to COE's network infrastructure and Websites.

To address vulnerabilities that could be exploited via the internet, we performed a penetration test on 205 servers residing in the COE that provided Web services to DOT personnel and the public. We also employed social engineering techniques on a random sample of COE users to assess their compliance with security awareness training.

Finally, we used a statistical sample of 134 out of 5,735 computers provided by COE's management to test for vulnerabilities. We were able to scan 99, or 73.9 percent, successfully resulting in an estimated universe of 4,237.[16] For those computers available at the time of testing, we found 34 (34.3%) out of our 99 computers had 86 Critical Issues. This statistical sample allowed us to project that our universe of 4,237 computers had 3,681 critical issues, within a 90 percent confidence level and a margin of error of 6.2 percentage points for the available computers. We used a NIST validated vulnerability assessment tool to determine whether the system had security weaknesses that could be exploited.

[15] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
[16] Our best estimate of 4,237 computers has a precision of +/-355 at the 90 percent confidence level.

EXHIBIT B. Related FISMA Recommendations

FISMA 2011: *Persistent Weakness In DOT's Controls Challenge The Protection and Security of Its Information Systems,* FI-2012-007, November 14, 2011.

Rec #	Status	Recommendation
2	Open	In conjunction with OA CIOs, establish incident monitoring and detection capabilities to include all of the Department's systems and facilitate central and real-time reporting.
5	Open	In conjunction with OA CIOs, verify that minimum security controls are adequately tested for deficient systems.

FISMA 2010: *Timely Actions Needed To Improve DOT's Cybersecurity,* FI-2011-022, November 15, 2010.

Rec #	Status	Recommendation
23	Open	Implement the use of PIV cards as the primary authentication mechanism to support multi-factor authentication at the system and application level for all DOT's employees and contractors.

FISMA 2009: *Audit of DOT's Information Security Program and Practices,* FI-2010-023, November 18, 2009

No	Status	Recommendation
16	Open	Ensure accurate information is used to monitor Operating Administrations' progress in correcting security weaknesses.

EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Nathan Custer	Program Director
Michael Marshlick	Project Manager
Felicia Moore	Information Technology Specialist
Jenelle Morris	Information Technology Specialist
Tracy Colligan	Information Technology Specialist
Nileshkumar Patel	Information Technology Specialist
Susan Neill	Writer-Editor
Megha Joshipura	Statistician

APPENDIX. AGENCY COMMENTS

Memorandum

U.S. Department of Transportation

Subject: ACTION: Response to the Office of Inspector General Draft Report on Common Operating Environment Security

Date:

To: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of:

From: Richard McKinney
Chief Information Officer

08/16/2013

DOT Focusing on Comprehensive Security Enhancements

The Office of the Chief Information Officer is making substantive changes to the Common Operating Environment (COE) to make the environment more secure for the systems it controls and operates, and for the systems it supports for the Operating Administrations (OAs) here at the Department. As the new CIO at DOT, I have committed to making cyber security the top priority. Improving our cyber security posture will require gaining the commitment of management and staff throughout the Department to make our cyber environment as safe and secure as possible. Getting the basics right is key to successfully achieving this goal so we are using a comprehensive team approach to planning and implementing the foundational elements along with developing longer term plans.

This renewed emphasis on having a secure environment acknowledges the significance of the OIGs findings, which we have already begun to address. While no open information technology (IT) environment can be completely safe from compromise, DOT has made great strides in making the COE environment safer with the addition of tighter controls, greater emphasis on continuous monitoring, and investing resources in better hardware and software. All our recent advancements balance the increasing risk threshold to DOT against the scarce resources at our disposal, but we will continue to balance the two competing forces to achieve our long term goals.

The Information Technology Shared Services (ITSS) organization has actions underway that meet or exceed the elements within the OIG recommendations. For example, the organization is working to better enforce Standard Operating Procedures (SOPs) for the Federal and contractor staffs supporting the COE, enforcing the Service Level Agreements (SLAs) with our OA partners to ensure both parties are fully aware and in compliance with the SLAs, and pulling the resources necessary to monitor our environment on a continuous basis to ensure the equipment connected to the COE is known or authorized. Additionally, the ITSS organization will more formally partner with the OAs and the DOT Chief Information Security Officer's (CISO) organization to look for ways to enhance security training throughout the Department and make all DOT employees more conscious of security risks and their role in maintaining a secure environment. Furthermore, I am committed to significantly increasing the number of staff assigned to the critical area of cyber-security in both the COE and the CISO office.

Coordinated ITSS and OA Effort Critical for COE Cyber Security Improvement

Achieving progress in improving the cybersecurity posture of the COE will require leadership by the ITSS organization along with coordinated and consistent cooperation from across the operating administrations. The COE is the government-owned, contractor-developed, and supported Government Services Solutions (GSS) that provides the OAs with common IT services such as identification and authentication domain requirements, file and print functions, messaging and directory capabilities such as electronic mail and web application access and database services. The COE's architecture provides a hosting environment for numerous major applications employed by the various OAs in support of their individual operational requirements. In addition, several applications necessary to support operations by all of the OAs have been integrated into the COE environment. The DOT Common Operating Environment consists of 4 major systems, Campus Area Network (CAN), Computing Services, Messaging Services, and Helpdesk Services. Comprehensive, cooperative and sustained efforts among all participants in the COE will be critical to the success of our endeavors;

Appendix. Agency Comments

Recommendation Prioritization

As a practical reality in light of the ongoing constraints on resources, and in order to align actions with our risk-based approach to cyber security, each of the responses to the OIG recommendations is accompanied by one of the following prioritization levels.

Ranking A: Recommendation will receive the highest priority and ITSS commits to work with the operating administrations to achieve the results within the timeframe specified.

Ranking B: ITSS will seek to include resources for action in upcoming budget cycles or reprioritize current year end funds, to the extent that they might become available. Implementation will commence only when funding is secured.

Ranking C: Based on the priority of compliance with direction from OMB, along with other priority use of funding and staffing, these actions would be addressed after priority A and B are completed or if there were an unexpected surfeit of funds.

One final note: the specific actions to implement the recommendations are described at a high level within the context of this document. More detailed action plans are being developed and will be shared separately with the OIG to avoid potential concerns with sensitive security information in this response.

Appendix. Agency Comments

RECOMMENDATIONS AND RESPONSE

[redacted] **Recommendation 1**: Enforce password complexity requirements [redacted] in accordance with Departmental Cybersecurity Compendium Order 1351.37.

[redacted] **Response**: Concur. ITSS management has reviewed [redacted] accounts to validate password complexity configuration settings. ITSS will:

- [redacted] Enforce password complexity requirements for any [redacted] which the COE creates in accordance with DOT policy.
- [redacted] Update standard operating procedures (SOP) for the COE [redacted] to include validation of password configuration setting compliance at least annually or whenever events occur (install, recovery, major change) to affect enforcement of DOT requirements.

This recommendation is considered priority ranking A. The first task outlined above will be completed no later than October 1, 2013. The second task, while still an A ranking, will take additional time and resources, but is planned for completion no later than March 31, 2014.

Recommendation 2: Monitor OAs periodic exercises that test COE users' knowledge of security requirements when accessing emails on the Government network.

Response: Concur. The CIO will collaborate with the OAs on enhanced security training programs that includes greater emphasis on topics such as spear phishing and other social engineering topics. ITSS will leverage these collaborative efforts and use these enhanced security training programs to help ensure full participation of the ITSS staff. In addition, ITSS will develop a security awareness communication plan that provides security information in multiple formats such as, emails and posters that bring additional attention to cyber security issues.

This recommendation is considered priority ranking A. The tasks outlined in this action are planned for completion no later than September 30, 2014.

Appendix. Agency Comments

Recommendation 3: Use automated tools, such as vulnerability scanners or Web application scanners to monitor applications residing in the COE on a constant basis, and require each OA to mitigate vulnerabilities in its system or remove the systems from the network.

Response: Concur. ITSS has adopted the DOT CISO developed and approved Security Authorization and Continuous Monitoring Guide 23 January 2013. To consistently address the recommendations, ITSS will:

- Coordinate regular web scans with the Cyber Security Management Center (CSMC) for identified web servers and applications;
- Issue a memorandum from the Associate CIO for ITSS to the OA CIOs, directing them to remediate or mitigate vulnerabilities in systems they administer that are connected to the COE.

This recommendation is considered priority ranking A. The tasks outlined in this action are planned for completion no later than March 31, 2014.

Recommendation 4: Develop and maintain a complete inventory (current registry) of authorized network devices (including wireless) accessible to staff who monitor departmental networks.

Response: Concur. The ITSS will maintain a registry of authorized devices on the COE network that can be provided at any point in time. Furthermore ITSS will take steps to minimize the risk of permitting unauthorized access to the COE by defining authorized devices, developing policy to add/remove devices from the COE network, and establishing procedures to identify and maintain an inventory of authorized devices on the COE network. ITSS will also turn down access to unused network connections by disabling ports. These actions provide an effective set of actions that can be implemented to fulfill the intent of this recommendation.

This recommendation is considered priority ranking A. The tasks outlined in this action are planned for completion no later than March 31, 2014.

As a supplemental action, ITSS will implement a robust Network Access Control (NAC) solution that would further prevent access to the COE network by unauthorized devices. This action is considered priority ranking B.

Appendix. Agency Comments

~~**FOR OFFICIAL USE ONLY. Public Availability To Be Determined under 5 U.S.C. 552, Freedom of Information Act.**~~

Recommendation 5: Ensure the system owners perform regular vulnerability assessments and scans of internal systems to identify known vulnerabilities and common
misconfigurations, and establish a practice to ensure that OAs and OCIO are collaborating and agreeing on remediation plans.

Response: Concur. The ITSS organization will partner with the OAs to develop remediation plans and identify known vulnerabilities and common misconfigurations. Additionally, ITSS will establish a practice to ensure OAs and OCIO are collaborating and agreeing on remediation plans.

Specifically, ITSS will:

- Coordinate with the DOT CISO and the CSMC to implement credentialed scans for the COE network, where COE provides the majority of support for the network;
- Implement a process to communicate identified vulnerabilities to appropriate OA personnel;
- Require OAs to provide status updates and remediation plans as part of the memorandum to be issued in response to Recommendation 3.

These processes are considered priority ranking A. The tasks outlined in this action are planned for completion no later than June 30, 2014.

In addition, as a supplemental action, ITSS will implement appropriate automated continuous monitoring capabilities to assess COE managed assets for vulnerabilities and configuration compliance. This action is considered priority ranking B.

Recommendation 6: Perform annual penetration testing as required by DOT policy.

Response: Concur. In compliance with DOT policy and the established Rules of Engagement (ROE) for penetration testing, the COE will engage an independent assessor to perform the testing.

This recommendation is considered priority ranking A. The task outlined in this action is planned for completion no later than March 31, 2014.

Appendix. Agency Comments

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review and respond to the report. If you have any questions concerning this response, please contact Thomas Jackowski, Acting Associate CIO for IT Shared Services, at (202) 493-0382.

Appendix. Agency Comments

~~**FOR OFFICIAL USE ONLY. Public Availability To Be Determined under 5 U.S.C. 552, Freedom of Information Act.**~~