Office of Inspector General

Audit Report

THE VOLPE CENTER'S INFORMATION TECHNOLOGY INFRASTRUCTURE IS AT RISK FOR COMPROMISE

The John A. Volpe National Transportation Systems Center

Report Number: FI-2016-056

Date Issued: March 22, 2016

~~FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.~~

Memorandum

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

Subject: **ACTION:** The Volpe Center's Information Technology Infrastructure Is at Risk for Compromise
The John A. Volpe National Transportation Systems Center
Report No. FI-2016-056

Date: March 22, 2016

George E Banks for

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

Reply to Attn. of: JA-20

To: Assistant Secretary for Research and Technology

The John A. Volpe National Transportation Systems Center (Volpe)—operating under the U.S. Department of Transportation's (DOT) Assistant Secretary for Research and Technology—provides research, development, and information technology (IT) services to Federal and State agencies, local entities, and partners abroad. These services include evaluating issues to assess transportation needs, performing engineering and safety analyses, and developing and providing innovative solutions. Currently, Volpe is assisting the Federal Aviation Administration with the Next Generation Air Transportation System.

In order to prevent unauthorized access to its customers' data and its own, Volpe's information network must be properly protected. We therefore conducted this self-initiated audit of the Center's information system security controls. Our objectives were to determine whether: (1) Volpe's local area network (LAN) and Web sites are secure from compromise, and (2) security weaknesses exist in Volpe's IT infrastructure.[1]

[1] IT infrastructure consists of hardware, software, networks, and facilities including buildings and data centers.

~~**FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.**~~

We conducted our work in accordance with generally accepted Government auditing standards. We reviewed Volpe's network documentation and security policies and performed assessments of Volpe's entire network, including penetration tests, vulnerability scans, and manual tests. We also interviewed Volpe personnel. See exhibit A for additional details on our scope and methodology.

RESULTS IN BRIEF

~~(FOUO)~~ Volpe's LAN is not secure from compromise. The National Institute of Standards and Technology (NIST) provides agencies guidance on protecting their networks from intrusions. However, we were able to gain access to many devices on Volpe's LAN because it did not follow NIST and DOT requirements. For example, Volpe used [redacted] and [redacted]. Volpe's use of [redacted] and [redacted] for [redacted] also made personally identifiable information (PII) vulnerable to compromise. We gained access to millions of PII records. Volpe also has not implemented comprehensive intrusion detection and prevention systems to ensure accurate detection of unauthorized access to its network. As a result, our testing went mostly undetected leaving the LAN exposed to unauthorized compromise.

~~(FOUO)~~ Some Volpe management practices create security weaknesses that make its IT infrastructure vulnerable to compromise. NIST's standards and DOT's security policy require Operating Administrations to scan for vulnerabilities in their information systems and hosted applications to identify and resolve system flaws. We found [redacted] on the LAN, indicating weaknesses in Volpe's scanning and remediation processes. Furthermore, Volpe's oversight practices for the network space it contracts out create a risk of compromise. The Center does not follow NIST's and DOT's policies and procedures for establishing agreements with clients that connect networks owned by third parties to its network. For example, the Federal Motor Carrier Safety Administration (FMCSA) has contracted with Volpe and has connections with third parties. Volpe had not required a security agreement with FMCSA regarding this connection. Furthermore, we identified vulnerabilities in the network space that Volpe hosts for DOT's Operating Administrations and [redacted]. Finally, Volpe does not maintain a complete inventory of its network devices. NIST's standards and DOT's security policy require Operating Administrations to maintain and regularly update inventories of their system assets (components and devices). However, Volpe's administrators do not have a complete inventory and cannot identify unauthorized devices. Consequently, Volpe's IT infrastructure and the systems and data on it are at risk for compromise. Volpe officials stated that these weaknesses are the result of security staff's limited oversight over vulnerability remediation, third party network connections, and inventory management.

We are making recommendations to assist the Assistant Secretary for Research and Technology in securing Volpe's IT Infrastructure.

BACKGROUND

To conduct its work, the Volpe Center partners with public and private organizations that also provide most of the Center's funding. Volpe maintains an information system infrastructure that provides network access to its employees, contractors, and the other Government agencies that the Center works with. Volpe's employees and contractors maintain the Center's information system security.

~~(FOUO)~~ As a method of recovering operating costs, Volpe contracts with partners, clients, [redacted], and other entities to provide network space. Under contract, these entities may use Volpe's network space to house project systems, work with third parties, and establish connections between networks owned by those parties and Volpe's network. Currently, FMCSA, the Navy's Maritime Safety and Security Information System and [redacted] have contracted to use space on Volpe's network for their own projects.

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

~~(FOUO)~~ Volpe classifies each of its systems as one of two types—institutional or project. Institutional systems include day to day business operation systems such as human resources, email, and business services such as telecommunications, computer workstations, and SharePoint services. Volpe's operations department manages the institutional systems. Project systems are research and development projects contracted by clients and partners. Project systems often include sensitive information such as data from [redacted] and PII. Volpe's research and technology department manages these systems.

In 2007, we reported that Volpe had not properly secured its network, not completed security evaluations, and not tested its contingency plans.

VOLPE'S LOCAL AREA NETWORK IS NOT SECURE FROM COMPROMISE

Volpe has not secured its LAN from compromise. The Center's security controls do not adequately protect the network and the PII it contains. Volpe also lacks comprehensive intrusion detection and prevention systems. These weaknesses increase the risk of unauthorized access and data loss.

Volpe's Network and Personally Identifiable Information Are Not Secure

~~(FOUO)~~ Volpe's network and PII are vulnerable to unauthorized access. Two practices have created this vulnerability: Volpe's use of [redacted] and [redacted] for [redacted] to systems for maintenance and updates; and [redacted] to network devices [redacted].

~~(FOUO)~~ NIST's standards and DOT's security policy require agencies to [redacted]—or [redacted] and [redacted] upon system installation. However, Volpe staff have not [redacted] for all [redacted]. Using [redacted] and [redacted] we gained access to two backup systems containing over 1,000,000 gigabytes of data.[2] The data in these systems include backups of network infrastructure servers, storage area networks, email, and the encrypted human resources database. We could have easily deleted this data from the systems. Volpe management stated that the loss of this data would be serious. If a business system also lost its data during an attack or disruption after the backups were lost, the data could be permanently lost.

~~(FOUO)~~ Furthermore, PII on Volpe's network is at risk for compromise because the Center has not implemented security safeguards that comply with DOT's security and privacy policies. DOT's Chief Information Officer Departmental Privacy Risk Management Policy requires that technical, physical, and

[2] A million gigabytes is also known as a petabyte. One petabyte could hold the entire printed works in the Library of Congress a hundred times over.

~~**FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.**~~

administrative safeguards be in place to protect the PII that the Department maintains. We accessed several [redacted] and PII on [redacted] [redacted] using [redacted] and [redacted]. We extracted over 4.2 million records including sensitive PII from an [redacted] [redacted] system.[3] The information included social security numbers, first and last names, dates of birth, birthplace, and addresses.

~~(FOUO)~~ Volpe security staff informed us that they had removed the [redacted] from the network, but our additional testing showed that the [redacted] were still on the network and the [redacted] and [redacted] had not been changed. Volpe management officials then informed us that these weaknesses result from security staff's lack of authority over the portion of Volpe's network dedicated to research projects. The management officials further stated that they lacked the necessary authority to hold system administrators accountable for mitigating this type of vulnerability. However, the lack of adherence to DOT's security policies, oversight, and accountability increases the risk of network compromise by unauthorized access. Those who gain unauthorized access could extract sensitive PII for identity theft, espionage, terrorism, or social engineering.

After we informed Volpe of these issues, the Center's information system security manager (ISSM) collaborated with the legal department to create a privacy risk management plan based on DOT and NIST guidance and regulations. Additionally, Volpe management officials informed us that in fiscal year 2016, they will expand the ISSM's authority to include the oversight of research project systems.

Volpe's LAN Is Vulnerable to Unauthorized Access

Volpe's security staff have not implemented comprehensive intrusion detection and prevention systems for the network to protect its IT infrastructure from unauthorized access. Intrusion detection systems (IDS) monitor and identify malicious traffic while intrusion prevention systems (IPS) also prevent intruders' malicious actions. NIST standards recommend that agencies use at least two types of intrusion detection and prevention systems together—host based and network based systems—to detect and prevent unauthorized access, denial of service attacks, viruses, and other threats. Host-based systems monitor traffic in and out of individual devices such as laptops, servers, and applications. Network-based

[3] ~~(FOUO)~~ [redacted]

~~FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.~~

systems monitor traffic over network infrastructure, including firewalls and routers. NIST standards further recommend usage of a network access control (NAC) solution to prevent unpatched, unauthorized and/or non-secure equipment from accessing network resources. Table 1 summarizes the status of Volpe's implementation of IDS, IPS and NAC.

Table 1. IDS, IPS, and NAC Implementation Status

System Type	Host/Network Based	Implemented
IDS		
	Host Based	Yes
	Network Based	No
IPS		
	Host Based	Yes
	Network Based	No
NAC Solution		
	Host Based	No
	Network Based	No

Source: OIG analysis

~~(FOUO)~~ Volpe management has implemented host-based IDS and IPS but no network-based IDS and IPS. As a result, security personnel cannot effectively monitor and review all network traffic. This lack of monitoring allowed our testing activities to go largely unnoticed. For example, we conducted several [redacted][4] attacks against different parts of the network and intercepted [redacted] as people [redacted]. A network IDS would have alerted Volpe's network security personnel that these attacks were happening. Volpe security personnel also cannot monitor traffic coming through trusted connections such as the inter-departmental network connection. [redacted] also has a direct connection to Volpe's LAN that is not monitored. This lack of monitoring recently allowed malicious software onto the LAN. Volpe's ISSM informed us that he is aware of the need for these detection systems but has lacked the personnel to implement a network based solution. Volpe's ISSM has hired new staff and is working on developing a solution.

Volpe management also has not implemented network access control which restricts access to a network by denying access to unpatched and unauthorized devices. The lack of this control allows a user to connect unauthorized devices to the network and as a result expose the network to compromise. Volpe management stated that the Center's previous implementation of network access

[4] ~~(FOUO)~~ [redacted]

control interfered with business operations. As an interim solution, they have focused on monitoring physical connections to the network, but the application they have in place is insufficient because it does not prevent devices plugged into the network from accessing network resources. Volpe officials informed us that to address this issue, they plan to implement a new solution[5] during the first quarter of fiscal year 2016.

~~(FOUO)~~ The Center's lack of comprehensive intrusion detection and prevention systems increases the risk that unauthorized activity on the network will go undetected. Furthermore, this lack of monitoring of the inter-departmental and [redacted] connections creates a risk that anyone with access to DOT's network can access these systems.

SOME VOLPE MANAGEMENT PRACTICES LEAVE ITS INFRASTRUCTURE VULNERABLE TO COMPROMISE

Some of Volpe's management practices leave the LAN vulnerable to compromise. Personnel do not resolve all the vulnerabilities that security scanning detects, and therefore, do not mitigate the risks for compromise that these vulnerabilities create. Volpe's lack of full oversight for the network space it provides to its clients increases the risk of compromise. Lastly, the Center does not maintain a complete inventory of its computer components and devices.

Volpe Does Not Resolve All the Vulnerabilities that Its Security Scanning Detects

Volpe management does not resolve all vulnerabilities detected during security scanning, and consequently, does not mitigate the risks of compromise that these vulnerabilities create. NIST defines a network vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. NIST also sets categories of vulnerability risk—low, moderate, and high—to systems. A low risk vulnerability is likely to have a limited adverse effect on a system, a moderate risk vulnerability is likely to have a serious adverse effect, and a high risk vulnerability is likely to have a catastrophic effect. NIST's standards and DOT's security policy require Operating Administrations to scan for vulnerabilities in their information systems and hosted applications to identify and resolve system flaws.

[5] An application called CISCO ISE that will automate and enforce context-aware security access to network resources, thus providing network admission control.

~~**FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.**~~

~~(FOUO)~~ Our scanning detected [redacted] of [redacted] and [redacted] in numerous system processes, servers, and other devices on Volpe's LAN. We found [redacted] and [redacted]. On the portion of the LAN that hosts Volpe's external Websites, we found [redacted] and [redacted]. For example, one server's out of date [redacted] had created a high level vulnerability that allowed us to take full, administrative control over the server. This level of access would allow an attacker to delete and steal data, install viruses and software, lock out administrators and use the server to attack additional servers on the network. Additionally, our vulnerability scans found [redacted] and [redacted] on database servers, printers, Web interfaces, and storage devices.

Volpe's personnel do not enforce remediation of vulnerabilities on project systems. Instead, they send copies of scan results to the system administrator for the device in question to remediate detected vulnerabilities. However, Volpe management does not have effective procedures and processes to enforce the remediation of these vulnerabilities. Additionally, Volpe security staff have an open POA&M regarding vulnerability scanning that has been open since October 2013. Volpe officials again informed us that these weaknesses are the result of security staff's limited oversight and lack of authority over the portion of the network dedicated to research projects. After we informed management of these deficiencies, the ISSM stated that security staff have started regular scanning for vulnerabilities on the network's research project segments.

Volpe management's lack of an effective process to enforce vulnerability remediation could lead to the exploitation of unpatched services, applications, and hardware.

Volpe's Lack of Full Oversight of Client Network Space Has Created IT Infrastructure Vulnerabilities

Volpe management has not established full oversight of its IT infrastructure including the space that it contracts for with clients. In addition, management has not defined security responsibilities in agreements with these clients to cover third-party connections to the LAN. Volpe has also not established client responsibilities for the systems clients have on Volpe's infrastructure. NIST's standards and DOT's policy require Operating Administrations to identify and document technical, security, and administrative responsibilities and formalize them in agreements with terms to which all parties agree.

The Center has not defined security responsibilities with clients that have established connections between its network and the third-party networks. For example, Volpe provides network space to FMCSA, and FMCSA has a connection with another party that connects to Volpe's network. Volpe and FMCSA have an interagency agreement that details Volpe's security responsibilities. However, this agreement does not specify responsibilities for FMSCA's third-party connection to Volpe's LAN. The Center has a POA&M open since October 2013 on this issue. Volpe management informed us that they originally believed that language in their interagency agreement with FMCSA was sufficient for the security of FMCSA's third-party connection, but during discussions with us, acknowledged that it is not.

~~(FOUO)~~ Furthermore, vulnerabilities in the systems hosted on space on the LAN that Volpe provides to FMCSA and [redacted] may also create risks for the LAN. FMCSA has declined Volpe personnel's security management and oversight specified in its interagency agreement with the Center. Volpe management informed us that they decided to allow FMCSA to manage its own security—despite the requirement in the interagency agreement for Volpe to fill this function—because of the value of the contract.

Because Volpe management has not established complete oversight for its IT infrastructure, including clear agreements with clients it contracts with for LAN space, it has created the possibility that these clients do not understand their responsibilities to mitigate security risks. Consequently, Volpe's whole IT infrastructure is at risk for attack from the client's systems due to their unknown vulnerabilities.

Volpe Does Not Maintain a Complete Inventory List of Its IT Assets

Volpe's inventory of its IT assets is incomplete. NIST standards and DOT's security policy require the development and documentation of a complete inventory of system components and devices that is regularly updated as installations, removals, and software updates are made.

~~(FOUO)~~ Volpe security staff conduct frequent scans of its network to determine what devices are connected. Weekly scans capture on average [redacted] out of the total [redacted] computing devices that we discovered between November 20, 2014 and March 27, 2015. Since Volpe management does not have a complete inventory list, it is impossible to determine whether all detected devices are actually authorized. There is a POA&M on the Center's information system inventory that has been open since October 2013.

Volpe management informed us that the Center does not have a comprehensive inventory in part because their limited oversight and authority over the network prevents them from developing a comprehensive inventory, and project teams can add assets to the network without the security staff's knowledge or approval. Volpe management also stated that the security staff plans to use DOT-provided technology to develop a solution.

Volpe management's lack of a complete inventory of network devices means that Volpe's security staff does not have an accurate view of the network and cannot identify unauthorized devices residing on the network. Consequently, the systems and data on Volpe's IT infrastructure are at risk for compromise.

CONCLUSION

~~(FOUO)~~ The Volpe Center provides important research and development and IT services to the Department's Operating Administrations, and State, local, and [redacted]. However, the Center has not adequately mitigated the risk of compromise in its networks and systems. Until Volpe fully establishes oversight and authority of its IT infrastructure and implements required NIST and DOT cybersecurity policies it cannot be assured that its systems are secure. Because of the breadth of its work, any vulnerabilities in the Center's own networks and systems put the systems of all its partners at risk for compromise as well.

RECOMMENDATIONS

~~(FOUO)~~ To improve computer security on Volpe's network and systems, we recommend the Assistant Secretary for Research and Technology require Volpe's Chief Information Officer (CIO) to:

1. Implement [redacted] procedures and policies in accordance with Departmental Cybersecurity Compendium Order 1351.37.

2. Implement security measures for protecting PII in accordance with DOT Chief Information Officer Departmental Privacy Risk Management Policy.

3. Install a network-based intrusion detection and prevention solution to complement the current host-based systems, enabling more comprehensive and accurate detection and prevention of malicious activity on the network, including traffic coming from trusted connections.

4. Implement a network admission control solution to ensure only authorized users can access network resources.

5. Conduct regular vulnerability assessments and scans of the LAN to identify known vulnerabilities and common misconfigurations, and implement a policy that holds system administrators accountable for remediating identified vulnerabilities.

6. Develop and execute interconnection security agreements with clients that it contracts with for network space on the IT infrastructure in accordance with NIST and DOT policy and guidelines.

7. Develop and maintain a complete inventory of authorized network devices accessible to staff who monitor departmental networks.

8. Implement a procedure to require the ISSM's approval before any device, including virtualized and other non-physical IT devices, is connected to the LAN, to include development and project systems.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided Volpe with our draft report on January 21, 2016 and received its response on February 18, 2016, which is included as an appendix to this report. Volpe concurred with our eight recommendations and provided appropriate actions and completion dates. Accordingly, we consider recommendations 1 through 8 resolved but open pending completion of the planned actions.

We appreciate the courtesies and cooperation of Volpe representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-4350, or Lou E. Dixon, Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-1427.

#

cc: DOT Audit Liaison, M-1
Volpe CIO, Eric Frykenberg
Volpe ISSM, Maurice Desruisseau
OST CIO, Richard McKinney
OST CISO, Andrew Orndorff

~~FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.~~

EXHIBIT A. SCOPE AND METHODOLOGY

We performed our network security assessment between September 2014 and September 2015, at DOT Headquarters in Washington, D.C., and the Volpe National Transportation Systems Center in Cambridge, MA. We conducted this audit 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.

The objectives of our security assessment of Volpe's network and infrastructure were to determine whether: (1) Volpe's local area network and Web sites are secure from compromise, and (2) security weaknesses exist in Volpe's information technology infrastructure.

To address our audit objectives, we used NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, to perform a penetration test and vulnerability assessment of the Volpe IT infrastructure using widely available tools and techniques.

We also interviewed Volpe management staff at the Center in Cambridge, MA, to determine what information and resources were critical to Volpe's operation and how protections were implemented. Our interviewees included Volpe's Deputy Director for Operations and Deputy Director for Research and Technology; Volpe's CIO and ISSM; and various Volpe IT staff. We also met with Volpe contractors from ActioNet and Nationwide IT Services.

We reviewed and analyzed documents, policies, and procedures related to Volpe's network infrastructure and Web sites using NIST 800-53 Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations.

EXHIBIT B. ENTITIES VISITED OR CONTACTED

DOT Agencies

- The John A. Volpe National Transportation Systems Center
- The Federal Motor Carrier Safety Administration

Volpe Contractors

- ActioNet
- Nationwide IT Services

EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Nathan Custer	Program Director
Daniel Joplin	Project Manager
Justin Ubert	IT Specialist
Zachary Lewkowicz	IT Specialist
Susan Neill	Writer-Editor
Tim Roberts	Senior Auditor
Petra Swartzlander	Senior Statistician

~~FOR OFFICIAL USE ONLY. Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552. Release to the public of contractor/grantee information contained in this report may be prohibited by the Trade Secrets Act, 18 U.S.C. § 1905.~~

APPENDIX. AGENCY COMMENTS

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

Assistant Secretary
for Research and Technology

1200 New Jersey, S.E.
Washington, D.C. 20590

February 17, 2016

Subject: INFORMATION: Management Response
Office of Inspector General (OIG) Draft Report-Volpe Center's
Information Technology Infrastructure is at Risk for Compromise

From: Gregory D. Winfree, Assistant Secretary for Research and Technology

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

The Department of Transportation (DOT) Office of the Assistant Secretary for Research and Technology (OST-R) and the Volpe Center (Volpe) remain fully committed to maintaining a secure environment for all Information Technology (IT) systems and data that Volpe manages. We continually strive to comply with Federal laws, directives, special publications, and Departmental policies and procedures. Given the importance of clearly delineating security roles and enforcing the remediation of vulnerabilities on project systems, going forward, Volpe's Chief Information Officer (CIO) and Information System Security Manager (ISSM) will engage with customers to clarify responsibilities for security oversight of IT systems tied to work performed for our customers. Volpe has already added staff to in anticipation of the additional level of effort that may be required to support customer needs.

Volpe has initiated additional actions in response to the findings and recommendations in OIG's draft report. Examples of efforts under way to strengthen information security include:

- ~~(FOUO)~~ Conducting weekly scans throughout the network, including searches for [redacted] settings. Volpe is implementing a more stringent audit process to confirm compliance with relevant network policies, to include [redacted] settings. Further, Volpe tracks and monitors all scan findings for remediation.

- Using a more comprehensive intrusion detection and prevention system for Volpe's network to ensure complete and accurate detection of unauthorized access. Volpe is also installing a system to mitigate network admissions control issue

- Developing and implementing, *Volpe Center Privacy Risk Management Program,* an operational guide based on DOT Privacy Order 1351.18 and NIST 800-53 Schedule J guidelines. Volpe's enhanced oversight efforts will also help to enforce the requirements of the program.

- Planning and developing a robust asset management program for Volpe Center network devices. The final Volpe Center Asset Management Plan will include a requirement that the ISSM office officially approve all devices before they are placed on the network.

Based on our review of the draft report, we concur with all eight OIG recommendations as written. Our target action dates for completing the recommendations are as follows:

Recommendations 1, 2, 3, 4, 5 and 8 to be completed by June 30, 2016.

Recommendations 6 and 7 to be completed by September 30, 2016.

We appreciate this opportunity to comment on OIG's draft report. Please contact Eric Frykenberg, Volpe Center CIO, at (617) 494-4810 and Maurice Desruisseau, Volpe Center ISSM, at (617) 494-2837, if you have any questions.