VOLPE CENTER'S INFORMATION TECHNOLOGY SECURITY AND RESOURCE MANAGEMENT ACTIVITIES

Research and Innovative Technology Administration

Report Number: FI-2007-061

Date Issued: August 1, 2007

Memorandum

U.S. Department of Transportation

Office of the Secretary
of Transportation
Office of Inspector General

Subject: ACTION: Report on Volpe Center's Information Technology Security and Resource Management Activities, RITA
Report Number FI-2007-061

Date: August 1, 2007

From: Rebecca C. Leng Rebecca Leng
Assistant Inspector General for Financial
and Information Technology Audits

Reply to
Attn. of: JA-20

To: Acting Research and Innovative Technology Administrator

This report presents the results of our audit on the effectiveness of information technology (IT) security and resource management activities at the John A. Volpe National Transportation Systems Center in Cambridge, Massachusetts.

A fee-for-service organization within the Department of Transportation's (DOT) Research and Innovative Technology Administration (RITA), the Volpe Center conducts research on critical transportation initiatives, such as aviation safety and Global Positioning System tracking for vessels and hazardous materials. In addition, Volpe provides operational support for vital DOT business operations, such as hosting the Federal Aviation Administration's (FAA) Enhanced Traffic Management System, DOT websites, and the implementation of the security access system for DOT's new Headquarters.

To support its user-fee operations, Volpe has established a complex network infrastructure.[1] Protected by security firewalls, this infrastructure provides interconnected networks and remote connections via the Internet for its 550 Federal employees and 850 contractor staff. Volpe personnel use these network computers to conduct sensitive research and develop new systems for customers. The network infrastructure also supports Volpe's administrative systems, such as e-mail and procurement management.

[1] A network infrastructure consists of a set of hardware and software used to interconnect computers and users, regardless of their physical locations.

Our objectives were to determine whether (1) Volpe's network infrastructure and connection entry points are adequately secured to protect the Center's critical information assets, (2) Volpe's information systems are properly accredited (secured) to support business operations, and (3) Volpe is leveraging departmental IT resources to maximize cost savings. We performed this audit in accordance with Generally Accepted Government Auditing Standards as prescribed by the Comptroller General of the United States and conducted such tests as we considered appropriate to detect fraud. Details of our scope and methodology are presented in Exhibit A.

RESULTS IN BRIEF

Volpe has established adequate firewall security to protect its IT infrastructure from intrusion or unauthorized access from the Internet. However, Volpe computers remained vulnerable to attacks by insiders—employees, contractor staff, and remote users from DOT's interconnected networks.[2] We found that Volpe's network vulnerability assessment was not effective in identifying security vulnerabilities and that network computers were not configured in accordance with departmental security standards to prevent weaknesses.

In addition, Volpe's system security certification review did not meet a key requirement. As part of this review, management must develop and test the system contingency plan to ensure continued operation in case of disaster. While Volpe reported that its systems have undergone such testing, the testing was limited to tabletop exercises—procedural walkthroughs. Volpe management has not yet tested its capability to resume system operations at its designated recovery site. In case of disruption due to power loss or disaster, both Volpe and customer systems might be affected.

Finally, Volpe has made good progress in leveraging departmental resources for more efficient operations. For example, it has converted its stand-alone financial and personnel/payroll systems to DOT's consolidated system solutions and is using the departmental enterprise licensing agreement to procure Oracle products for cost savings. We, however, identified two additional opportunities warranting management attention. First, Volpe was not included in the Department's enterprise license agreement and had to negotiate its own licensing agreement with Microsoft. In addition, Volpe, along with several other DOT Operating Administrations are paying separate license fees for using a software company's procurement system. Consolidating these operations with the Department could enable Volpe to further reduce costs.

[2] In March 2007, Volpe added firewall security between the DOT Headquarters and Volpe networks.

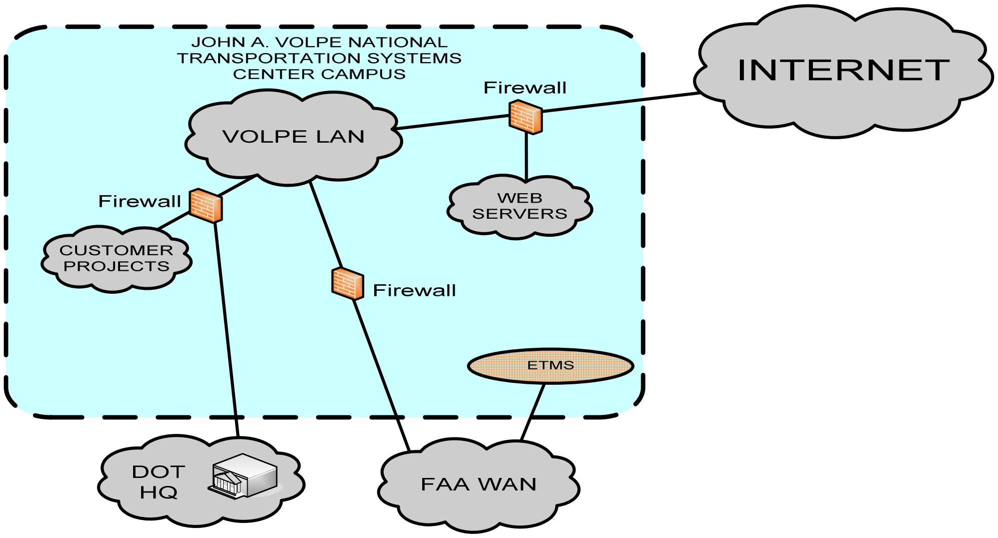
We provided a draft of this report to RITA for comment on May 15, 2007, and on July 18 we received the Agency's response. RITA concurred with our conclusions and stated that the majority of the recommendations have already been either fully or partially addressed. The response further stated that comprehensive plans are being developed for the completion of all remaining issues. A complete set of our recommendations can be found starting on page 9 of this report. RITA's response can be found in its entirety in the appendix.

FINDINGS

Volpe's Network Infrastructure Was Not Properly Secured and Remained Vulnerable to Attack by Insiders

While Volpe had adequate security protection to prevent unauthorized access from the Internet, its network remained vulnerable to attack by insiders, including employees, contractors, and remote users from DOT's interconnected networks. The Volpe network infrastructure consisted of its data center (which housed critical information systems); devices controlling the network connection to DOT's Headquarters, FAA, and the Internet; and computers used to conduct research or develop customer systems (see figure 1).

Figure 1. Current Volpe Network Infrastructure



Source: OIG based on Volpe data

Volpe's Network Vulnerability Assessment Was Not Effective in Identifying Security Weaknesses

Volpe management relies on a contractor to scan its network, including web servers, to identify vulnerabilities for correction. These vulnerability assessments were infrequent—only on a quarterly basis—and too limited in scope. Conversely, DOT performs vulnerability scans on its major systems, such as DOT websites and internal networks, on a weekly basis. Scanning for network vulnerabilities on a quarterly basis is not frequent enough to identify potential weaknesses, considering that new vulnerabilities are discovered virtually on a daily basis. According to the National Institute of Standards and Technology (NIST), during January 2007 alone, more than 300 new vulnerabilities were found on various commercial software products.

The assessment performed by the contractor was also too limited in scope to provide security assurance. The contractor's assessment in May 2006 identified 47 high-risk vulnerability incidents on about 90 computers. We performed independent assessments in May and November 2006, and discovered more than 8,800 potential vulnerability incidents—over half high-risk—on 412 affected computers and network printers (see table 1).[3]

Table 1. Volpe Center Network Vulnerability Incident Assessment Results

Equipment	Total Number of Hosts Tested	Number of Hosts With Vulnerabilities	Potential Vulnerability Incidents			Total Potential Vulnerability Incidents
			High	Medium	Low	
Computers	1170	397	2598	509	3802	6909
Network printers	88	15	1848	33	73	1954
Total	**1258**	**412**	**4446**	**542**	**3875**	**8863**

Source: OIG

As acknowledged by Volpe management, one computer could contain multiple incidents of the same vulnerability. For example, using weak passwords to authenticate users is a vulnerability because they could be easily cracked or guessed. If five users were found to use weak passwords to gain access to one computer, five vulnerability incidents would be included in table 1. We are

[3] High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium-risk and low-risk vulnerabilities may provide attackers with useful information, such as password files, that they can then use to compromise a computer system.

reporting the total number of vulnerability incidents because multiple incidents require multiple corrections.[4]

By using the vulnerabilities identified on 15 database systems deployed for project development, we were able to take full control of 7 systems, including those used to develop the Advanced Retrieval (Tire, Equipment, Motor Vehicles) Information System (ARTEMIS).[5] We could have corrupted the data stored in these systems or launched denial-of-service attacks to disrupt the development work.

Network Computers and Databases Did Not Meet DOT Security Configuration Standards and Were Not Adequately Reviewed

DOT policy[6] requires all computers to be configured in compliance with departmental minimum security standards. Yet according to Volpe officials, such standards were not previously enforced and are now being implemented only on newly deployed computers. Existing systems' configurations were not checked by Volpe to ensure compliance. In fact, the vulnerabilities we identified were largely caused by improper configuration.

Also, the security certification and accreditation (C&A) review performed in 2004 on Volpe's network infrastructure, known as the General Support System/Local Area Network (GSS/LAN), was too limited. It did not cover all key components used to support Volpe's missions.

For example, the risk assessment was conducted at the data center and did not cover other key areas of Volpe's LAN, such as the network connection to the Internet and computers that were used to support and maintain its networks. Without performing a full assessment of its entire network infrastructure—the most complex and vital system—Volpe cannot be assured that it is providing an adequate level of security protection to its business operations.

Network Security Weaknesses Could Adversely Affect Volpe's Business Operations

It is important that appropriate security controls be in place to protect the Volpe Center's critical IT infrastructure and information assets, which are used to support Volpe's user-fee operations. In 2006, Volpe had 424 projects underway, with annual obligations totaling about $262 million. More than 60 percent of the

[4] According to Volpe, there were a total of 1,838 potential vulnerabilities—359 high, 534 medium, and 945 low—for the 8,863 incidents identified during the audit.

[5] This system is used by the National Highway Traffic Safety Administration to collect and categorize product data, as well as death and injury data submitted by manufacturers, to identify potential tire defects in order to prevent any additional vehicle-related injuries and deaths.

[6] DOT IT and Information Assurance Policy 2006-04, April 3, 2006.

projects were for DOT customers. The rest were for other Federal agencies, state and local governments, the private sector, and international entities (see table 2).

Table 2. Volpe Customer Projects in 2006

Customers	Number of Active Projects	Total New Obligation Authority Transferred to Volpe ($ in millions)
DOT		
FAA	74	$81.9
Others	196	$88.7
Non-DOT		
Other Federal Agencies	126	$88.4
State/local Government	16	$2.0
Private sector	8	$0.3
International	4	$0.6
Total	**424**	**$261.9**

Source: Volpe

Any potential security weaknesses could jeopardize the confidentiality, integrity, and availability of Volpe's services to its customers. Further, its interconnectivity with DOT networks means that security weaknesses on Volpe's network could compromise DOT computer systems or vice versa, which, in turn, could potentially limit the Department's ability to conduct its vital business to support our national transportation system.

According to Volpe and RITA management, security weaknesses in network assessment and computer configuration were caused primarily by significant staff turnover at the Volpe Center. During the last 2 years, Volpe had to fill its chief information officer (CIO) position four times, which led to restructuring of duties within the CIO's office on several occasions. This high rate of turnover required its key personnel to assume multiple roles and responsibilities that were loosely defined, resulting in inadequate procedures for network vulnerability assessment and lax oversight of contractor work to provide adequate network security.

Volpe is in the process of recertifying the security protection of the GSS/LAN and must ensure that the review covers all network components at the Volpe Center. In response to our identified vulnerabilities, Volpe acted immediately to correct the confirmed high-risk vulnerabilities and review the remaining ones. According to Volpe officials, over 75 percent of high-risk vulnerabilities were corrected. In addition, Volpe management has hired a new contractor to perform ongoing assessments of its network vulnerabilities and recently drafted new operating procedures to direct the contractor's network vulnerability assessment work.

Security Evaluation for an Operational System Was Not Completed, and Contingency Plans To Recover Critical System Operations Were Not Tested

The Department requires Operating Administrations to report systems used to support agency missions in the official systems inventory and conduct systems security C&A reviews of these systems before they become operational. After that, system security needs to be re-certified every 3 years or upon major changes to the system. Security certification reviews provide senior management with the assurance that the information systems they rely on are meeting the minimum Government security standards to ensure the integrity, confidentiality, and availability of business operations.

Security Evaluation Not Complete

Volpe depends on five information systems to support its missions. We found that it omitted two systems from the official systems inventory and did not complete the required security certification review on one of the systems it did identify, called the Facility Physical Security System (see table 3).

Table 3. Volpe Systems Inventory

System	Included in Systems inventory?	Received Security Certification Review?
General Support System/LAN	Yes	Yes
Administrative Support	Yes	Yes
Procurement	Yes	Yes
Data Warehouse	No	Yes
Facility Physical Security	No	No

Source: OIG based on DOT and Volpe data

Volpe relies on the Facility Physical Security System to control access to various parts of the building, including areas housing sensitive research work. The system has been in operation for 3 years. According to Volpe management, it initiated the security C&A review of this system in January 2006; however, it has not yet completed the review. Once this system's C&A review is complete, the system will be able to be relied upon to control physical access to the Volpe facility.

System Contingency Plan Not Tested

As part of the security C&A review, management must develop and test the system contingency plan to ensure continued operation in case of disaster. While Volpe reported that its systems have undergone such testing, we found that the testing was limited to tabletop exercises—procedural walkthroughs. Volpe management has not yet tested the capability to resume system operations at its designated recovery site.

In addition to the five systems used to support its mission, Volpe houses customer systems for other DOT Operating Administrations and one non-DOT entity. The customer service agreement between Volpe and these customers specifies whether Volpe or the customer is responsible for disaster recovery. At least one DOT customer has asked Volpe to be responsible for developing and testing the contingency plan for the customer's system.

Should the Volpe data center become nonfunctional due to loss of power or a disaster, both Volpe and the customer's business operations would be disrupted. To mitigate this risk, Volpe signed an agreement with a commercial vendor to use the vendor's facility as the systems recovery site. However, 3 years after signing the agreement, Volpe has never conducted on-site testing to ensure that systems could indeed be recovered at the vendor's site in a timely manner.

In May 2006, Volpe conducted limited testing of the network connectivity between the systems recovery site and the alternate work site, where key Volpe personnel would be relocated in case of disaster. However, the network capacity established during the test only supported two customer systems and did not cover all Volpe systems at the recovery site in case of disaster. Accordingly, all Volpe and customer systems and associated business operations remain at risk. After we brought this concern to Volpe management's attention, we were informed that Volpe plans to conduct full recovery testing in August of this year.

As stated above, Volpe has experienced a significant gap in its IT leadership and high turnover rates among key staff in recent years. As a result, contingency plan testing was overlooked and there has been a lack of progress in reviewing, testing, and certifying that the Facility Physical Security System is adequately secured to support Volpe operations.

Volpe Is Using Departmental IT Resources for Cost Savings, but More Can Be Done

The Presidential Electronic-Government (e-Gov) initiative aims to facilitate the cost-effective acquisition of all goods and services and requires Federal agencies to consolidate common and general support services. In recent years, Volpe has made good progress in consolidating its common IT operations by leveraging departmental resources. For example, it has converted its stand-alone financial and personnel/payroll systems to DOT's consolidated system solutions. In addition, Volpe has utilized the departmental enterprise licensing agreement to procure Oracle software for cost savings. However, we found two areas that warrant management attention.

First, the Department has negotiated an enterprise licensing agreement that would provide savings on the acquisition of Microsoft products. However, Volpe management was not aware of the departmental license with Microsoft. According to Volpe management, this was largely due to Volpe's frequent staff turnover. Between November 2004 and November 2005, Volpe negotiated its own agreements to acquire 1,810 licenses of Microsoft products and later acquiring an additional 700 licenses in 2007 for a total cost of $224,000. Due to different contract terms in the departmental and Volpe licensing agreements, we were unable to assess the potential cost savings had Volpe utilized the departmental licensing agreement to procure the 2,510 licenses for Microsoft products. However, the departmental agreement was structured to save money on large quantities of software purchases. Therefore, Volpe should work with the Department and in the future utilize DOT licensing agreements.

Second, Volpe is using a commercial procurement system marketed by CompuSearch, called PRISM, with an annual license fee. Meanwhile, several other DOT Operating Administrations also use this commercial procurement system and are paying CompuSearch separate license fees. In FY 2005, the Department identified potential cost savings by consolidating Operating Administrations' use of this commercial system.[7] However, according to Department officials, this consolidation effort has been suspended due to a lack of funding. We plan to follow up on this issue with departmental management; therefore, we are not making any recommendations on this issue at this time.

RECOMMENDATIONS

We recommend that the Acting RITA Administrator direct the Volpe Director to:

1. Strengthen Volpe network security by:

   a. Assigning a high priority to correcting remaining high-risk vulnerabilities identified on Volpe computers during our audit and establishing a timetable to remediate all other vulnerabilities.

[7] OIG report "Office of the Chief Information Officer's Budget," Report Number FI-2005-055, March 31, 2005.

b. Finalizing the procedures for network vulnerability scanning and remediation and ensuring that they are properly implemented by the contractors.

c. Fully implementing the Department's security configuration standards for commercial software products operating on all Volpe computers.

d. Ensuring that all critical network infrastructure components are included in the current security certification review of the General Support System/Local Area Network.

2. Enhance protection of systems in operation by:

a. Completing the security certification and accreditation review of the Facility Physical Security System and ensuring that all systems are included in the Department's official systems inventory for tracking and management review.

b. Conducting systems recovery testing at the back-up site for Volpe and for customer systems for which it is responsible.

c. Testing network connectivity between the system recovery site and the alternate work site to ensure that network capacity can fully support Volpe business operations.

3. Achieve cost savings by working with the Department's Chief Information Officer to ensure that Volpe is given an opportunity to participate in and utilize future Department-wide enterprise software licensing agreements.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

A draft of this report was provided to RITA for comment on May 15, 2007, and on July 18 we received the Agency's response, which can be found in its entirety in the appendix. RITA concurred with our conclusions and stated that the majority of the recommendations have already been either fully or partially addressed. The response further stated that comprehensive plans are being developed for the completion of all remaining issues.

The corrective actions that RITA and the Volpe management have taken, and plan to take, adequately address the intent of our recommendations. Management responses to our recommendations are summarized below:

Recommendation 1.a: RITA concurred. All identified vulnerabilities that were related to software updates or patching were remediated. The remaining vulnerabilities requiring system reconfigurations will be corrected by June 2008, and those requiring system replacements will be completed by September 2009.

Recommendation 1.b: RITA concurred. The vulnerability scanning and remediation process has been updated in compliance with DOT standards. The new process assigns responsibility of monitoring and remediation to individual systems owners: both Volpe Center institutional assets and projects. Currently, Volpe is using the Foundstone Enterprise scan tool to track remediation efforts and provide oversight to ensure compliance.

Recommendation 1.c: RITA concurred. The Volpe Center is now deploying all new file servers, workstations, and laptops in accordance with DOT security configuration standards. The task of upgrading the existing file servers, workstations, and laptops to DOT's 2007 security standards will be completed by September 2008. Remaining issues that can only be corrected with system replacement will be corrected by September 2009.

Recommendation 1.d: RITA concurred. The current Volpe LAN/GSS C&A review package will include all critical network infrastructure components. The review will be completed by October 30, 2007.

Recommendation 2.a: RITA concurred. The C&A review of Facility Physical Security System will be completed by October 30, 2007. Volpe will also include all systems in DOT's system inventory by July 31, 2007.

Recommendation 2.b: RITA concurred. Off-site COOP and disaster recovery exercise will be completed by October 30, 2007.

Recommendation 2.c: RITA concurred. Network connectivity testing of Volpe institutional systems will be conducted as part of the COOP exercise to be completed by October 30, 2007.

Recommendation 3: RITA concurred. The Volpe Center and the Office of the Secretary have agreed that the Volpe Center will be included in all future DOT Microsoft enterprise license agreements.

ACTIONS REQUIRED

RITA's actions taken and planned satisfy the intent of our recommendations, subject to follow-up provisions in DOT Order 8000.1C. We appreciate the courtesies and cooperation of the Research and Innovative Technology

Administration, especially Volpe Center representatives, during this audit. If you have any questions concerning this report, please contact me at (202) 366-1496 or Edward Densmore, Program Director, at (202) 366-4350.

#

cc: Director, Volpe Center
Chief Information Officer, DOT
Chief Information Officer, RITA
Martin Gertel, M-1
Dilcy Garro, RTV-1

EXHIBIT A. SCOPE AND METHODOLOGY

The audit field work was performed between May 2006 and March 2007 at the Volpe Center in Cambridge, Massachusetts, and RITA Headquarters in Washington, D.C. The audit was conducted in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to provide reasonable assurance of detecting fraud, abuse or illegal acts.

We examined the underlying network infrastructure supporting Volpe missions, including Internet entry points, remote access connections, and the private network. In addition, we reviewed Volpe firewall configuration files and security policies and procedures. Using commercial network scanning tools and other commonly available software utilities, we performed two network scans that covered Volpe's internal network and critical network devices such as firewalls and routers. We also performed limited internal penetration testing to validate the identified vulnerabilities.

We reviewed Volpe's certification and accreditation documents, continuity of operations plans, IT systems inventory, and plan of actions and milestones. We also visited the Center's back-up and alternate work sites located in Massachusetts.

Finally, we reviewed Volpe's IT procurement practices for major hardware and software applications and DOT's existing enterprise licensing and blanket purchase agreements.

We interviewed key officials, including systems owners, network and database administration officials, and senior management.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Edward Densmore	Program Director
Dr. Ping Z. Sun	Project Manager
Henry Lee	Senior Computer Scientist
Aaron Nguyen	Computer Scientist
Vasily Gerasimov	Information Technology Specialist
Atul Darooka	Information Technology Specialist
Michael P. Fruitman	Communications Adviser
Harriet Lambert	Writer-Editor

APPENDIX. MANAGEMENT COMMENTS

U.S. Department
of Transportation
**Research and
Innovative Technology
Administration**

The Administrator

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

July 18, 2007

INFORMATION MEMORANDUM TO THE INSPECTOR GENERAL

From: John A. Bobo, Jr., Acting Administrator JAB
(202) 366-7582

Thru: Curtis J. Tompkins, Director, Volpe Center
(617) 494-2222

Prepared by: C. Eric Frykenberg, Chief Information Officer, Volpe Center
(617) 494-4810

Re: Volpe Center Response to Draft OIG Audit of Volpe Center's Information Technology Security and Resource Management Activities

SUMMARY

This memorandum is provided in response to the Office of Inspector General's (OIG) request for the Research and Innovative Technology Administration/Volpe National Transportation Systems Center (RITA/Volpe Center) management comments and statement of actions to be taken on the OIG's "Draft Report on Audit of Volpe Center's Information Technology Security and Resource Management Activities" provided on July 16, 2007.

Many work hours were expended by the Volpe Center staff and OIG audit team during the May 2006 to November 2006 time-frame of the audit. RITA/Volpe Center considers the OIG audit to have been an overall positive and beneficial process and appreciates the contributions of all personnel involved.

Remediation of all issues raised is a top priority for RITA and the Volpe Center. The majority of report recommendations have already been either fully or partially remediated and comprehensive plans are being developed for the completion of all remaining issues.

RITA provides the following status update on the OIG recommendations.

1. Strengthen Volpe Center Network Security by:

a. Assigning a high priority to correcting remaining high risk vulnerabilities identified on Volpe Center computers during our audit and establishing a timetable to remediate all other vulnerabilities.

Volpe Center response: Concur
Status: The Volpe Center has remediated all software updates and/or security patching vulnerabilities identified in the IG scan. All vulnerabilities requiring system reconfigurations will be corrected by June 2008, and all vulnerabilities requiring system replacement will be completed by September 2009.

b. Finalizing the procedures for network vulnerability scanning and remediation, and ensuring that they are properly implemented by the contractors.

Volpe Center response: Concur
Status: The vulnerability scanning and remediation process has been updated since the IG inspection and is now compliant with DOT standards. The Volpe Center now has a more comprehensive process in place that assigns responsibility for monitoring and remediation to individual system owners. This includes both the Volpe Center institutional assets and projects. The Foundstone Enterprise scan tool now allows the Volpe Center to track remediation efforts and provide oversight to ensure compliance.

c. Fully implementing the Department's security configuration standards for commercial software products operating on all Volpe Center computers.

Volpe Center response: Concur
Status: The Volpe Center is now deploying all new file servers, workstations, and laptops in accordance with DOT security configuration standards. The task of upgrading the existing installed base of all file servers, workstations, and laptops to DOT's 2007 security standards is an extensive project. All system reconfigurations will be completed by September 2008. Remaining issues that can only be corrected with system replacement will be corrected by September 2009.

d. Ensuring that all critical network infrastructure components are included in the current security certification review of the General Support System/Local Area Network.

Volpe Center response: Concur
Status: The current LAN/GSS Certification and Accreditation package will include a comprehensive assessment of all critical network infrastructure components.
Expected completion date is October 30, 2007.

2. Enhance protection of systems in operation by:

a. Completing the security certification and accreditation review of the Facility Physical Security System and ensuring that all systems are included in the Department's official systems inventory for tracking and management review.

Volpe Center response: Concur
Status: Certification and accreditation of Facility Physical Security System (termed Security Access System (SAS) will be completed by October 30, 2007.

b. Conducting systems recovery testing at the backup site for Volpe Center and for customer systems for which it is responsible.

Volpe Center response: Concur
Status: Off-site Continuity of Operations Plan (COOP) and Disaster Recovery (DR) exercise to be completed by October 30, 2007.

c. Testing network connectivity between the system recovery site and the alternate work site.

Volpe Center response: Concur
Status: On May 17, 2006, the Volpe FMCSA project successfully conducted a DataComm test of remote connectivity between the SunGuard cold site and the SunGuard hot site. Network connectivity testing of Volpe institutional systems will be conducted as part of the COOP exercise to be completed by October 30, 2007.

3. Achieve cost savings by working with the Department's Chief Information Officer to ensure that the Volpe Center is given an opportunity to participate in and utilize future Department wide enterprise software licensing agreements.

Volpe Center response: Concur
Status: The Volpe Center fully supports utilization of DOT enterprise software licensing agreements. The Volpe Center and OST have agreed that the Volpe Center will be included in all future DOT Microsoft enterprise license agreements. The Volpe Center is already included in all other DOT enterprise license and blanket purchase agreements such as Oracle, Safeboot, eTrust, and Dell.

The following pages contain textual versions of the graphs and charts found in this document. These pages were not in the original document but have been added here to accommodate assistive technology.

Volpe Center's Information Technology Security and Resource Management Activities

Section 508 Compliance Presentation

Figure 1. Current Volpe Network Infrastructure

The diagram shows the network infrastructure:

- A firewall connecting Volpe LAN, Web Servers and Internet.
- A firewall connecting Volpe LAN, Customer Project networks and DOT headquarters.
- A firewall connecting Volpe LAN and FAA WAN.
- FAA WAN is connected to ETMS network.
- Volpe LAN, Customer Projects, Web Servers and ETMS are within the border of the John A. Volpe National Transportation Systems Center Campus.

Source: OIG based on Volpe Data

Table 1. Volpe Center Network Vulnerability Incident Assessment Results

- 397 of 1170 computers were found having vulnerabilities. A total of 6909 potential vulnerability incidents were identified: 2598 high, 509 medium, and 3802 low.
- 15 of 88 network printers were found having vulnerabilities. A total of 1954 potential vulnerability incidents were identified: 1848 high, 33 medium, and 73 low.
- Total 412 of 1258 hosts (computers and network printers) were found having vulnerabilities. A total of 8863 potential vulnerability incidents were identified: 4446 high, 542 medium, 3875 low.

Source: OIG

Table 2. Volpe Customer Projects in 2006

- DOT customer FAA has 74 active projects with a total of $81.9 million new obligation authority transferred to Volpe.
- DOT other customers have 196 active projects with a total of $88.7 million new obligation authority transferred to Volpe.
- Non-DOT other federal agencies have 126 active projects with a total of $88.4 million new obligation authority transferred to Volpe.

- Non-DOT state/local government clients have 16 active projects with a total of $2 million new obligation authority transferred to Volpe.
- Non-DOT private sector clients have 8 active projects with a total of $0.3 million new obligation authority transferred to Volpe.
- Non-DOT international clients have 4 active projects with a total of $0.6 million new obligation authority transferred to Volpe.
- Total number of active projects for all customers is 424 with a total new obligation authority transferred to Volpe is $261.9 million.

Source: Volpe

Table 3. Volpe Systems Inventory

- General Support System/LAN was included in the systems inventory and received security certification review.
- Administrative Support system was included in the systems inventory and received security certification review.
- Procurement system was included in the systems inventory and received security certification review.
- Data Warehouse system was not included in the systems inventory but received security certification review.
- Facility Physical Security system was not included in the systems inventory and did not receive security certification review.

Source: OIG based on DOT and Volpe data