SECURITY OF THE FEDERAL RAILROAD COMPUTER SYSTEMS NETWORK

Federal Railroad Administration

Report Number: FI-2006-029
Date Issued: January 9, 2006

Memorandum

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

Subject: ACTION: Report on Audit of Security of the Federal Railroad Computer Systems Network FI-2006-029

Date: January 9, 2006

From: Theodore P. Alves
Principal Assistant Inspector General for
Auditing and Evaluation

Reply to Attn. of: JA-20

To: Federal Railroad Administrator

This report presents the results of our audit of the security of the network infrastructure at the Federal Railroad Administration (FRA). FRA relies on this network infrastructure[1] and the information stored in its computers to conduct its safety inspection mission and other critical functions, such as analyzing rail economics, identifying rail defense issues, and routing hazardous materials. Securing FRA's network infrastructure is critical to both the Department of Transportation (DOT) and FRA missions because FRA is one of the Department's five Operating Administrations (OAs) that have direct connections to the Internet. Each OA is responsible for securing its own Internet connection.

In 1996 FRA moved out of the DOT Headquarters building due to environmental issues. It subsequently established its own network connections to the Internet to support its Washington and regional office operations. The Agency uses firewall[2] and virtual private network (VPN)[3] technologies to secure these connection points. FRA has also established remote dial-up (telephone line) connections to support hundreds of inspectors who travel across the country performing railroad safety inspections, such as examining railroad tracks. Through these telephone lines, inspectors, who include 180 state inspectors, access information stored in the FRA

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

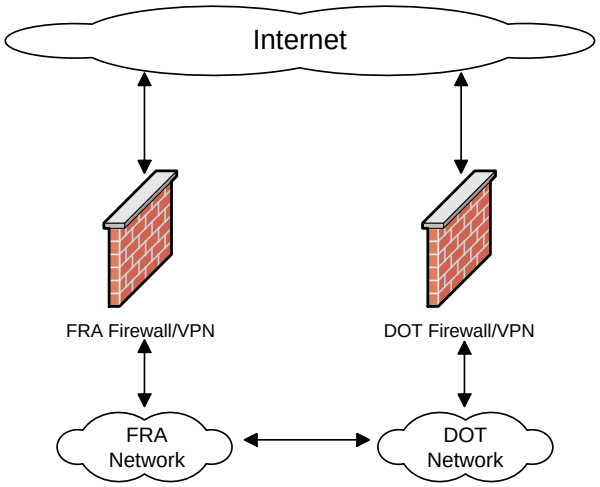
[2] A firewall is a network device located at an Internet entry point. It serves as the first line of defense against cyber attacks from the Internet and prevents unauthorized access to an agency's private networks.

[3] The *virtual private network (VPN*) technology provides remote users with secure access to an organization's network on a public or shared telecommunications infrastructure such as the Internet.

safety database and submit their inspection results, including proposed penalties for safety violations.

Over the past 4 years, the Office of Inspector General has conducted a series of computer security reviews at DOT Headquarters and field offices of several OAs. These reviews have revealed many network security weaknesses that could cause disruptions to not only individual OAs but also to the rest of the Department because of DOT's interconnected networks (see the Figure).

Figure. DOT's Interconnected Networks



The objective of this audit was to determine whether FRA's network infrastructure is adequately secured to support both DOT and FRA missions. Specifically, we sought to determine whether FRA's (1) network computers are properly configured and monitored to reduce the risk of attack, (2) Internet entry points are adequately protected to prevent cyber attack, and (3) remote network entry points used by employees and state inspectors are properly secured to prevent unauthorized access.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards as prescribed by the Comptroller General of the United States and performed such tests as we considered necessary to detect fraud, waste, and abuse. Details of our scope and methodology are discussed in Exhibit A.

RESULTS IN BRIEF

Overall, the FRA network was vulnerable to unauthorized access and attack from both inside and outside the Department. For example, during the audit, our staff was able to gain unauthorized access to FRA's individual computers from the Internet and obtained sensitive information[4] from these computers. In addition, we were able to take control of a network switch managed by FRA, and the main telephone switch maintained by the Office of the Secretary of Transportation (OST) for FRA. We could have changed the configuration in these switches to shut down a portion of the network or telecommunications service and cause serious disruption so that safety inspectors could not perform their work. To illustrate this concern, we changed the emergency contact telephone number in the telephone switch to one in the Office of Inspector General. This activity was not detected because FRA had not fully implemented an intrusion-detection monitoring capability.

Given its interconnectivity with other DOT networks, FRA's lack of security also put other departmental systems at risk. This was caused by a combination of lax management oversight, the absence of formal security policies and procedures,[5] and the absence of a full-time security official to oversee and enforce systems security.[6] Now that an official with responsibility for information systems security oversight is in place, it is critical that FRA assign a high priority to enhancing the network security it has lacked but clearly needs.

We are providing specific recommendations to better protect computers on the network, enhance the capability of detecting security breaches, increase personnel security, and strengthen management oversight. FRA management agreed with our recommendations and has started taking corrective actions.

The following summarizes what we found.

The FRA network was vulnerable to unauthorized attack from both inside and outside the Department. Computers on the FRA network had many vulnerabilities, some of which had been previously reported to FRA management but remained uncorrected. Our independent assessment revealed additional critical weaknesses not previously identified. These enabled us to gain unauthorized access to FRA computers from the Internet, including root-level access over a critical file server, desktop computers, and a network switch. From

---

[4] For security reasons, specifics concerning the weaknesses and vulnerabilities we identified and our audit procedures are not discussed in this report but were provided to FRA managers during the audit.

[5] FRA currently has draft security policies and procedures going through the final stages of formal coordination with FRA offices.

[6] The FRA Information System Security Officer (ISSO) position was vacant from June 2004 through April 2005, 2 months after we began this review in February 2005. During that time, the Director of the Office of Information Technology was the Acting ISSO.

these computers we obtained sensitive information. FRA management is taking aggressive actions to eliminate all high-risk vulnerabilities.

About 65 percent of FRA employees connect remotely to FRA's network, which supports FRA's safety mission efficiently since its inspectors have to perform railroad safety inspections, such as examining railroad tracks, throughout the country. However, this high percentage of remote users creates a challenge for FRA's network security. About half of all FRA computers are not subject to routine vulnerability checks because they are being used by employees remotely the majority of the year. These unchecked computers, if infected with hostile software, could become conduits for spreading problems to the rest of FRA and other DOT networks.

Another security concern is that FRA granted 180 state inspectors access to its network without checking with state agencies to determine whether these personnel had received proper background investigations. While such investigations provide no guarantee of a person's loyalty or trustworthiness, they do provide some valuable information that might keep some personnel who pose a risk to DOT security from working on DOT systems.

FRA's Internet connections were not adequately secured. To secure a computer network, management needs to not only patch or eliminate vulnerabilities in computers but also install additional tools, commonly known as intrusion-detection systems, to monitor traffic throughout the network for potential security breaches. This detection control is especially critical to networks with direct connections to the Internet because of relentless attacks by hackers worldwide. FRA procured an intrusion-detection system in September 2002 and certified that this control had been implemented in September 2003. However, we found that FRA did not start deploying this control until June 2005, after we made inquiries about it. FRA explained that this critical investment was idle for so long because of the lack of technical expertise by the existing contractor personnel. FRA management has committed to fully deploying this essential control.

While FRA's reliance on firewall security and VPN technology to control access to its private network from the Internet focused on the right technologies, these tools were not properly managed. First, FRA did not remove a former firewall administrator's (a contractor) root-level access privileges to the firewall software for 6 months. Second, FRA forgot to remove the VPN connection to another contractor's office after the contractor had completed the task. As a result, FRA left open two paths through which unauthorized individuals could gain access into its private network from the Internet. Both security vulnerabilities were corrected after we brought them to FRA management's attention. To prevent the recurrence of such problems, FRA needs to develop a firewall security policy detailing

criteria for granting access from the Internet and requiring periodic evaluation of the firewall and VPN configuration by the Information System Security Officer.

FRA network was vulnerable to unauthorized remote access. In addition to using VPN connections, FRA employees and state inspectors can also access the FRA network via dial-up modem connections. FRA has established a central modem pool to control such access with mandatory user authentication. However, it also allowed use of more than 50 separate dial-up lines outside of central modem pool control. FRA could not provide justification for or locate most of these dial-up lines. Through an unsecured line, we were able to dial into FRA's main telephone switch and successfully change its configuration. This vulnerability could cause serious disruption to FRA's telecommunications operations. FRA took immediate action working with OST to secure the telephone switch after we brought this issue to management's attention.

Another form of remote access that has gained significant popularity in recent years is wireless technology. This technology can be used to transmit data to and from remote locations. Since wireless connections bypass traditional security mechanisms on wired networks, such as firewalls or VPNs, they have to be monitored carefully. FRA did not allow the use of this technology within its network infrastructure at the time of our audit; nevertheless we found an active wireless entry point within FRA Headquarters. This entry point was not connected to the FRA network and, therefore, did not impose a direct threat. However, we were concerned that FRA management did not know about this entry point. The access point was removed after we brought it to FRA's attention. The lack of oversight of these remote connections was partially due to turnover of key security staff.

FINDINGS

FRA Computer Network Was Vulnerable

Computers on the FRA network had many vulnerabilities, which had been known for months, if not years. Our independent assessment revealed additional critical weaknesses that were not previously identified. Together, these weaknesses enabled our audit staff to gain unauthorized access to individual FRA computers from the Internet and take control of part of its network infrastructure.

We also identified two other concerns. First, about half of all FRA computers are not subject to routine vulnerability checks because they are used by employees remotely. These unchecked computers, if infected with hostile software, could become conduits for spreading problems to the rest of FRA and DOT networks.

Second, FRA granted 180 state inspectors access to its network but did not verify with state agencies whether these inspectors had received proper background investigations.

Known Security Vulnerabilities Not Corrected

Using commercial scanning software, we performed a vulnerability assessment of the FRA network and found over 2,400 high-risk, 1,000 medium-risk, and 15,800 low-risk security vulnerabilities[7] on 448 computers hosted at FRA Headquarters and regional offices. Some of these vulnerabilities are well known in the hacker community, such as blank passwords, using the default manufacturer's passwords, or weak passwords. We gained total control (root-level access) of a critical file server, desktop computers, and a network switch. We obtained sensitive business information and could have made unauthorized configuration changes to these computers, including installing malicious software.

- *Critical file server*. This server allowed us to obtain critical network infrastructure information. By using this information, we were able to gain unauthorized access to FRA computers directly from the Internet.
- *Desktop computers used by FRA employees*. These computers yielded sensitive safety and personnel information.
- *A network switch (a computer networking device that connects network segments).* By taking control of this switch, we were in a position to reconfigure the FRA network—including shutting down a portion of it.

Some of these vulnerabilities had been known to FRA for months, if not years. The DOT Transportation Cyber Incident Response Center (TCIRC) has been providing weekly vulnerability scans of FRA private networks since 2003. For example, a high-risk vulnerability we found was identified by TCIRC weekly scans in January 2005. In fact, this same vulnerability was also identified in the FRA systems security certification and accreditation document dated June 2003.

FRA's inaction in correcting these known vulnerabilities was caused by the lack of operating procedures and management oversight of contractor performance. According to FRA officials, it relied on a contractor to review and correct these vulnerabilities. The contractor started working with FRA in November 2004 but had left by June 2005. The turnover of key contractor personnel caused delays in corrective actions.

---

[7] 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 an attacker with useful information, such as password files, that they can then use to compromise a computer system.

While our independent assessment found vulnerabilities similar to those identified by TCIRC, we also found additional significant weaknesses. For example, we identified other types of weak passwords associated with root-level user accounts, while TCIRC scans did not. FRA should work with TCIRC to expand its weekly scans.

FRA management is acting to eliminate all high-risk vulnerabilities and is developing a timetable for correcting those that remain.

Hundreds of FRA Computers Not Checked for Vulnerabilities

We identified a disparity in the number of FRA computers that were being scanned by TCIRC and the total number of computers on the network. We reviewed the TCIRC scanning results on six occasions during January and February 2005. During these scans, the number of FRA computers varied. The average number of FRA computers identified during each scan was less than 500, as shown in the following table. Yet FRA has more than 1,000 computers. Therefore, about half of all FRA computers were not subject to routine network security checks by TCIRC.

Table. TCIRC Scanning Results

Date Scanned	No. of Computers Scanned
2/16/05	550
2/09/05	545
1/31/05	371
1/26/05	565
1/17/05	323
1/07/05	380
Average per scan	456

FRA's high percentage of remote users explains the discrepancy. About 65 percent of FRA employees are remote users. Many safety inspectors connect to FRA's network remotely the majority of the year because they have to perform railroad safety inspections, such as examining railroad tracks, throughout the country. They use laptops to submit their inspection reports to the safety database hosted on the FRA network. When off the network, these computers cannot be reached during the scans. These laptops, if infected with hostile software such as

viruses, spyware, or Trojan horses,[8] could become conduits for spreading problems to the rest of the FRA network and other DOT networks. Currently, FRA has no procedure in place to ensure that these computers are being adequately secured and patched to prevent cyber attack.

No Assurance of Background Checks on Hundreds of State Inspectors

FRA did not inquire with state agencies as to whether the 180 state inspectors given access to the FRA network had received proper background checks. This was allowed to occur because of a lack of proper management oversight. These state inspectors were given access to a sensitive safety database on the FRA network. Some of these inspectors also have active accounts in the FRA e-mail system. According to DOT policy, non-DOT personnel—contractors, industry associates, or other Government employees—are subject to the same background check requirement as DOT employees before they are allowed to access DOT systems. FRA should immediately contact cognizant state agencies for this information and remove the access privileges of those without proper background checks.

Internet Entry Points Were Not Adequately Secured

FRA did not start implementing the intrusion-detection system that it procured in September 2002 until June 2005. Installing this security is especially critical to organizations with direct connections to the Internet because of relentless attacks by hackers worldwide. Annually, FRA invests about 50 percent of its total IT budget in its IT infrastructure. FRA explained that this critical investment was idle for so long because contractor personnel lacked technical expertise.

FRA relies on firewall security and a VPN to secure its Internet connection points. However, we found two incidents in which these technologies were not properly managed. First, FRA did not remove a former firewall administrator's (a contractor) root-level access privileges to the firewall software for 6 months. Second, FRA forgot to remove the VPN connection to another contractor's office after the contractor had completed the task. Both security incidents were corrected after we brought them to FRA management's attention.

---

[8] Viruses, spyware, and Trojan horses are software programs capable of replicating themselves and causing substantial damage to a computer. A *virus* is a program that infects computer files, usually executable programs, by inserting a copy of itself into the file. There copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate. *Spyware* refers to software that monitors user activity without user knowledge or consent. A *Trojan horse* is a computer program that conceals harmful code; it usually masquerades as a useful program that a user would want to execute.

Intrusion-Detection System Not Implemented in a Timely Manner

Intrusion detection is the process of detecting unauthorized use of or attack on a computer or network. Intrusion-detection systems are software or hardware systems that detect such misuse. The National Institute of Standards and Technology recommends deploying such systems as necessary additions to an organization's security infrastructure. This security is particularly important to organizations with direct connections to the Internet because of constant hacking attacks.

FRA has spent about $500,000 to acquire and maintain a suite of security software, including an intrusion-detection system (IDS), since September 2002. The certification and accreditation document for the FRA network, certified in September 2003, stated that "a network-based IDS is in place and is currently monitoring the network for attacks and Internet abuse by internal users." However, we found that the implementation of the intrusion-detection system had not begun until June 2005, after we inquired about it. FRA management explained this critical investment was idle for so long because contractor personnel lacked technical expertise. FRA has committed to fully deploying the intrusion-detection system promptly.

Until the intrusion-detection system is fully deployed, FRA cannot effectively protect its computers in today's volatile network environment. Other DOT OAs that have installed intrusion-detection systems have reported hundreds or thousands of potential security breaches daily.

Firewall Security and VPN Connections Not Properly Managed

We found a security weakness in FRA's firewall configuration. A former firewall administrator (a contractor) still had root-level access to the firewall software after having transferred to another position 6 months previously. With this access, the former administrator could continue modifying the firewall configuration, including opening additional unauthorized pathways to get into the FRA network from the Internet.

Use of VPN technology has become increasingly popular in recent years because it provides secure connections on public networks, such as the Internet, which is more economical than private networks. Because 65 percent of FRA employees remotely connect to its network, FRA has begun allowing its employees, contractors, and state inspectors to access its private network from the Internet using VPN technology. The number of VPN users at FRA more than doubled during our audit. The VPN connection to a contractor's office was not properly managed.

- About a year ago, FRA authorized a contractor to establish a VPN connection to the FRA network for a specific task. However, FRA did not remove this connection after the contractor had completed the task. As a result, people working in that contractor's office could continue accessing the FRA network on the Internet.

- FRA did not obtain security assurance from this contractor that the contractor's network was configured to meet DOT security requirements and that only authorized personnel could use the connection to access the FRA network. The Department requires OAs to obtain such security assurances from outside parties before allowing them to be connected to DOT.

Both access paths were removed after we brought the issues to FRA management's attention. These incidents happened because FRA has not developed a firewall security policy and did not have a procedure with which to periodically evaluate the firewall and VPN configuration. DOT requires that each OA develop a firewall policy and use it as a baseline for configuring its firewall so that only legitimate network traffic can enter the protected networks. In addition, a designated Information System Security Officer (ISSO) should periodically review and approve all access and configuration changes made to the firewall and VPN. However, FRA did not have a full-time ISSO until April 2005. With the new security officer on board, FRA should assign a high priority to enhancing its network security.

FRA Network Vulnerable to Unauthorized Remote Access

In addition to using VPN connections, FRA employees and state inspectors can access the FRA network via dial-up modem connections. Beyond its central modem pool, FRA allowed people to use more than 50 separate dial-up lines. Use of these dial-up lines was neither justified nor secured, in most cases. We also found an active wireless entry point at FRA Headquarters. While this entry point was not connected to the FRA network and did not impose a direct threat, we were concerned that FRA management did not know about its existence.

Dial-Up Connections Were Not Justified or Secured

FRA provided us with a list of 57 dial-up numbers that were authorized for use to make connections to the network. However, FRA could neither explain what these individual dial-up lines were intended for, nor justify why employees were allowed to use these telephone line connections, bypassing central modem pool controls.

We were able to determine that 2 of the 57 dial-up lines were reserved for testing purposes, and 1 was used for FRA Headquarters' main telephone switch maintained by OST. However, the dial-up line to the telephone switch was not secured. Anyone could use that telephone number to dial into the main telephone switch.

By using the unsecured dial-up connection and the default user password, we were able to alter the configuration in the main telephone switch, including system diagnostics, notification, and memory settings. For example, we changed the emergency contact telephone number to the main number of the Office of Inspector General without being detected.

By using these combined weaknesses, hackers could disrupt FRA telecommunications services, which could lead to major disruptions in business operations. FRA has taken action, working with OST, to secure the dial-up line to its telephone switch and has agreed to disable the remaining 54 dial-up lines.

Wireless Connection Found

DOT requires that each wireless device that is used to process or store DOT data or that connects to a DOT network, must be approved for use by the designated official. According to FRA management, it neither used nor supported wireless connections to its network at the time we conducted the audit. However, we found an active wireless access point at FRA Headquarters. Later, FRA management informed us that the access point had been used to test wireless technology and should have been disconnected after the test.

We confirmed that the wireless entry point was not connected to the FRA network; therefore, it did not impose a direct threat to FRA. However, we were concerned that FRA management was not aware of the existence of this wireless access point, which could be easily connected to the FRA network and become an unsecured path. After we brought the issue to management's attention, the access point was located and removed.

The lax management oversight of these remote connections was partially due to the turnover of key security staff. FRA did not have a full-time Information System Security Officer until April 2005. Before that, the position was filled on an acting basis by someone with other primary responsibilities. With a full-time Information System Security Officer, who should report periodically to FRA's Chief Information Officer, FRA should assign a high priority to enhancing its network security.

RECOMMENDATIONS

We recommend that the FRA Administrator direct the FRA Chief Information Officer to:

Enhance FRA network security by:

1. Eliminating all high-risk vulnerabilities identified in FRA computers within 30 days and establishing a timetable to correct the remaining vulnerabilities.

2. Ensuring that timely actions are taken to correct vulnerabilities identified in future weekly scanning reports.

3. Developing a mechanism to ensure that all computers used remotely are periodically checked for vulnerabilities and patched with the latest security upgrades.

4. Contacting state agencies to find out whether the 180 state inspectors given access to the FRA network have received proper background checks and establishing a target date to disable their access if the requested information is not received.

Strengthen security at Internet connection points by:

5. Fully deploying the intrusion-detection system to monitor traffic on the FRA network promptly.

6. Developing a firewall policy commensurate with DOT security requirements.

7. Establishing procedures to ensure periodic evaluation of firewall and VPN configuration by the Information System Security Officer.

8. Requiring that security assurance be obtained from outside entities before allowing them access to FRA's private networks through VPN connections.

Prevent unauthorized remote access by

9. Disabling the remaining 54 dial-up connections to the FRA network.

10. Establishing procedures to periodically detect unauthorized wireless access points on the FRA network infrastructure.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

A draft of this report was provided to the Federal Railroad Administrator for comments on October 27, 2005. FRA's Deputy Administrator responded on November 21, 2005, and concurred with all recommendations. For security reasons, we are not including FRA's written response in our report due to the specificity of the agency's statements. However, its response is summarized below.

The actions taken and planned by FRA are generally reasonable. However, no target date was provided for recommendation 4 and management's response to recommendation 9 indicates that FRA may not disable all 54 dial-up connections. If FRA does not disable all of these connections, management should justify the need to use them and ensure that they are adequately secured. Specific comments by FRA and its planned actions on our recommendations are provided below.

Recommendation 1: FRA concurred. FRA has committed to eliminating the outstanding risks promptly.

OIG Response: The action taken and planned by FRA meets the intent of our recommendation.

Recommendation 2: FRA concurred. FRA will institute written processes that will ensure timely corrective actions to resolve identified vulnerabilities promptly.

OIG Response: FRA's planned action meets the intent of our recommendation.

Recommendation 3: FRA concurred. FRA will promptly develop a plan to ensure that all computers used remotely are regularly checked for vulnerabilities and patched with the latest security upgrades.

OIG Response: FRA's planned action meets the intent of our recommendation.

Recommendation 4: FRA concurred with exploration of alternative solutions. FRA determined that out of the 30 participating programs, only 7 States perform any type of background check on inspectors. FRA proposes limiting the access of State program personnel who have not undergone some type of background check to Internet email only. These users will not have access to FRA's private network including safety inspection systems.

OIG Response: FRA's planned action partially addresses our recommendation. The response did not specify how many State inspectors have received proper background checks in accordance with DOT policies. Further, the response did

not provide a target date to disable State inspectors' access to FRA's private network if evidence of proper background checks is not received.

Recommendation 5: FRA concurred. FRA has committed to promptly deploying the intrusion-detection system.

OIG Response: FRA's planned action meets the intent of our recommendation.

Recommendation 6: FRA concurred. FRA indicated they developed and instituted a firewall policy commensurate with DOT security requirements in November 2005.

OIG Response: FRA's action meets the intent of our recommendation and will be subject to a follow-up review.

Recommendation 7: FRA concurred. FRA's Information System Security Officer has committed to establishing procedures to ensure periodic evaluation of firewall and VPN configuration by December 15, 2005.

OIG Response: FRA's planned actions meet the intent of our recommendation.

Recommendation 8: FRA concurred. In November 2005, the FRA Office of Information Technology indicated they developed and instituted a formal VPN process, which requires users to sign a VPN end-user agreement prior to obtaining VPN access.

OIG Response: FRA's action meets the intent of our recommendation.

Recommendation 9: FRA concurred in part. FRA has committed to promptly disconnecting any remaining unused dial-up connections.

OIG Response: Based on conversation with FRA officials, they indicated that FRA may not disable all 54 dial-up connections. In that case, management should justify the need to retain the dial-up lines and ensure that they are adequately secured.

Recommendation 10: FRA concurred. FRA indicated they started conducting periodic checks of unauthorized wireless access points in November 2005.

OIG Response: FRA's planned action meets the intent of our recommendation and will be subject to follow-up review.

ACTIONS REQUIRED

In accordance with Department of Transportation Order 8000.1C, we request that FRA provide within 15 days, the number of inspectors without proper background checks and a target date for disabling their access to FRA's private network (Recommendation 4). We also request that FRA provide information on the number of dial-up lines that are retained and secured (Recommendation 9).

We appreciate the courtesies and cooperation of FRA representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1992 or Rebecca C. Leng, Assistant Inspector General for Information Technology and Computer Security, at (202) 366-1488.

cc: Chief Information Officer, DOT
Chief Information Officer, FRA
Martin Gertel, M-1
Victor Angelo, RAD-43

EXHIBIT A. SCOPE AND METHODOLOGY

We reviewed the underlying network infrastructure supporting FRA missions, including Internet entry points, remote access connections, and the private network. Specifically, we used commercial scanning software and other commonly available scanning tools to identify network hardware (routers, firewalls, concentrators, dial-up modems) and system software configuration vulnerabilities that allowed unauthorized access to the FRA network. We did this network scanning from the internal networks at FRA Headquarters and a regional office. We interviewed key network administration officials and reviewed FRA firewall configuration files and security policies and procedures to ensure adequate enforcement.

Additionally, we assessed FRA wireless and VPN usage, two relatively new and popular technologies used by many Federal agencies. We used wireless scanning software to identify the wireless access points and evaluated whether the security used to protect them was adequate. We also reviewed the VPN hardware and software configuration to ensure that the settings adhered to current industry standards and procedures. In addition, we performed limited penetration tests on VPN connections by exploiting identified vulnerabilities.

Our audit work was performed between February and August 2005 at FRA Headquarters in Washington, DC, and a regional office in Cambridge, Massachusetts. 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 waste, fraud, or abuse.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Rebecca C. Leng	Assistant Inspector General for Information Technology and Computer Security
Edward Densmore	Program Director
Dr. Ping Z. Sun	Project Manager
John Johnson	Senior Information Technology Specialist
Aaron Nguyen	Computer Scientist
Michael P. Fruitman	Communications Adviser