Office of Inspector General

Audit Report

Headquarters Computer Network Security

Department of Transportation

Report Number: FI-2000-124
Date Issued: September 25, 2000

Memorandum

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

Subject: **INFORMATION:** Report on Headquarters Computer Network Security, DOT
FI-2000-124

Date: September 25, 2000

Reply To
Attn Of: Meche:x61496

From: John L. Meche
Deputy Assistant Inspector General for Financial, Information Technology, and Departmentwide Programs

To: Chief Information Officer, DOT

This report is the second in a series on our audit of the Department of Transportation (DOT) headquarters telecommunications network security[1]. These headquarters computer networks are used to support transmission of critical administrative and financial data such as payroll, grant payments, safety statistics and research information throughout DOT. The objectives of the audit were to determine whether: (1) adequate controls are established to prevent, detect, and respond to unwanted Internet access to DOT headquarters networks; (2) sensitive information on DOT headquarters networks is protected with access authentication and secure transmission; and (3) network performance is properly monitored.

The first report[2] in the series recommended corrective action concerning personnel security for employees of the Federal Government and contractors. In this report, we determined whether DOT computer systems are adequately secured to prevent unwanted access by Internet users and whether web servers, which are computers containing information accessible by Internet users, are properly configured to reduce the risk of attack. We plan to issue the third report addressing network transmission control and performance monitoring in the near future.

[1] For security reasons, specifics concerning the computer networks and our audit procedures are not discussed in this report, but were provided to DOT managers during the audit.

[2] Interim Report on DOT Computer Security, Report Number: FI-2000-108, July 13, 2000.

RESULTS IN BRIEF

DOT has interconnected private networks that are to be restricted to authorized users. To protect its private networks, DOT established a small public network as a "neutral zone" to house public web servers between its private networks and the Internet. We found DOT headquarters computer networks had security weaknesses that made its computers and web servers vulnerable to unauthorized access and attack by intruders. Specifically:

- DOT computers were accessible by unauthorized Internet users. We gained unauthorized access from the Internet to about 270 computers located within DOT's private networks. These computers were located throughout DOT, but none was within the Federal Aviation Administration (FAA) or U.S. Coast Guard Headquarters. DOT strengthened its network security during our audit and agreed to take additional corrective actions.

- DOT computers were vulnerable to insider attack--another source of intrusion threat. While DOT headquarters network computers have been given added protection against unauthorized Internet access as a result of our audit, we found about 900 computers located throughout DOT internal agencies could be accessed by unauthorized insiders, such as employees, contractors, and grantees. Our prior reviews identified vulnerabilities to attack and abuse by insiders. For example, we identified over 600 contractor employees, who were no longer working for DOT, still retained authorized access to DOT systems[3]. After we identified this issue, management removed thousands of access authorizations. Our work also resulted in the prosecution of employees who embezzled funds through stolen passwords, including one who embezzled $600,000 from DOT. DOT management agreed to disable unneeded network services on these computers, and to develop procedures to prevent recurrence.

- Internet users were allowed to bypass DOT's "firewall"[4] security and gain access to DOT's private networks because 13 public web servers were inappropriately placed on DOT's private networks. DOT management corrected this weakness during our audit by moving these web servers to a separate network area or outside of DOT networks, and has agreed to reiterate its policy to prevent recurrence.

---

[3] FAA Computer Security Controls of Data Processing Center, Report Number: FE-1999-103, May 20, 1999.

[4] A firewall is a set of related computer programs located at a network gateway computer. Based on a set of rules, a firewall screens Internet users' requests. Then the computer takes action to accept or reject access into a private network, or to direct requests to public viewing web sites.

- DOT web sites were vulnerable to attack. DOT has about 240 web servers for public access through its Home Page. Of the 119 web servers reviewed, we identified a total of 111 vulnerabilities on 67 web servers. The vulnerabilities are categorized into three risk levels--41 rated as high, 16 rated as medium, and 54 rated as low risks.[5] DOT management is correcting these vulnerabilities, and strengthening configuration controls over web servers.

These weaknesses could be avoided with better firewall security, stronger enforcement of Internet security requirements specified by the DOT Chief Information Officer (CIO), and additional management controls over the configuration (computer setup) of web servers. Until the computer industry improves security designs, users' best protection is through stringent controls over Internet connections; adequate configuration management controls, such as turning off unnecessary network services installed by computer manufacturers; and prompt installation of computer manufacturers' security software fixes and upgrades.

Personnel from the CIO Office stated that they are trying to allocate more resources to enforce internal agencies' compliance with DOT Internet security requirements. For Fiscal Year (FY) 2000, the CIO Office has only one employee designated to enforce information security. In April 2000, the CIO Office received additional funding of $296,000 for contract support and procurement of a network monitoring tool. The CIO Office requested $1.1 million and $3.6 million for information security for FYs 2001 and 2002, respectively. However, personnel from the CIO Office stated that they may have to reassess the funding needed to implement our recommendations.

BACKGROUND

Computer security is getting increased attention due to Presidential Decision Directive 63, which calls for protecting the Nation's critical infrastructure by May 2003. DOT has over 600 mission-critical systems operating on DOT's private networks, and over 240 web servers that it encourages the public to access from the Internet through the DOT Home Page. DOT relies on network security software—firewalls—to direct network traffic from the Internet into either DOT's private networks (for authorized users) or to public viewing web sites.

The Federal Government is using the Internet more extensively for day-to-day functions, such as e-mail and information exchange. Congress also requires Government agencies to provide the option of electronic maintenance, submission, or disclosure of information as a substitute for paper by October 2003. As the

[5]A high vulnerability may provide an attacker with immediate access into a computer system, such as executing commands on a web server. Medium vulnerability may provide information that has a high potential of giving system access to an intruder, such as getting a password file. Low vulnerability may provide information that potentially could lead to a compromise, such as providing a user name.

Government extends its Internet use to more critical applications, there are more opportunities for cyber intrusions. Recent denial-of-service attacks on e-commerce sites and e-mail systems have served as "wake-up" calls for enhancing Internet security. Recognizing this, the President issued directives to all Federal agencies aimed at strengthening Internet security.

SCOPE AND METHODOLOGY

DOT has thousands of computers on its private networks and about 240 public web servers that are accessed through the DOT Home Page by millions of Internet users. We used questionnaires sent to headquarters network managers to gather background information on the DOT headquarters networks. We reviewed documents on network security policies, network design diagrams, plans and procedures, security assessments, and contingency plans.

We interviewed key network administrative officials and used a commercial software scanning tool to assess vulnerabilities on DOT headquarters network computers. We scanned about 16,000 DOT computers to identify installed network services, such as modems and web servers. We also scanned about 1,100 computers and 119 public viewing web servers to assess security vulnerabilities. This audit was limited to headquarters networks and did not include wide area networks supporting nationwide operations within FAA and Coast Guard.[6]

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Audit work was performed between November 1999 and August 2000 at DOT, FAA, and U.S. Coast Guard Headquarters in Washington, D.C.

ANALYSES AND RESULTS

To access DOT networks, Internet users can use many communications tools. The Hypertext Transfer Protocol (HTTP)[7] web browser is the most frequently used tool—providing about 95 percent of Internet access to DOT networks. Accordingly, our audit focused on evaluating whether DOT computers are adequately secured to prevent unauthorized Internet access with a web browser. We found DOT computers were vulnerable to unauthorized access.

[6] These include various networks used to support administrative, air traffic control, and search and rescue operations. These networks will be reviewed in future audits.

[7] HTTP is a set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the Internet.

Security Needs to be Strengthened to Prevent Access by Unauthorized Internet Users

Office of Management and Budget (OMB) Circular A-130 "Management of Federal Information Resources" requires Federal computer systems to be secured from unauthorized access. DOT Order H1350.2 "Information System Security Program" (Internet policy) requires that network computers be accessible only to authorized users. DOT uses a firewall, at network entry points, to protect against unauthorized access from the Internet. However, our test found that the firewall configuration allowed unauthorized Internet traffic to pass through the firewall to DOT's private networks.

By using a commercial software scanner, we scanned about 16,000 computers connected to DOT headquarters networks which are used to process and transmit critical administrative and financial data such as payroll, grant payments, safety statistics, and research information throughout DOT. Our scanning identified about 1,300 computers with active HTTP web services (a software program handling web browser access requests). Among the 1,300 computers, about 550 are used at FAA and Coast Guard Headquarters and the remaining 750 are used by other DOT internal agencies.

By logging on as a non-DOT Internet user and using a web browser commonly installed on home computers, we performed a web accessibility test on the 1,300 computers. We were unable to gain access from the Internet to about 1,030 computers, including all FAA and Coast Guard Headquarters computers. However, we gained unauthorized access to about 270 computers in 10 of DOT's internal agencies.

Weak firewall security and a lack of enforcement of access security requirements in the Department allowed the unauthorized access. During the audit, we brought this matter to the attention of the CIO staff who agreed to strengthen firewall security by restricting Internet users' access. As of August 3, 2000, the firewall allowed Internet access via the HTTP service to only two computers on DOT's private networks. While user identification and password authentication are used to control access to these two computers, user identification and passwords are not encrypted when transmitted over the Internet. Internet access to these two computers needs to be secured.

Unneeded Network Services Need to be Eliminated to Prevent Access by Unauthorized Insiders

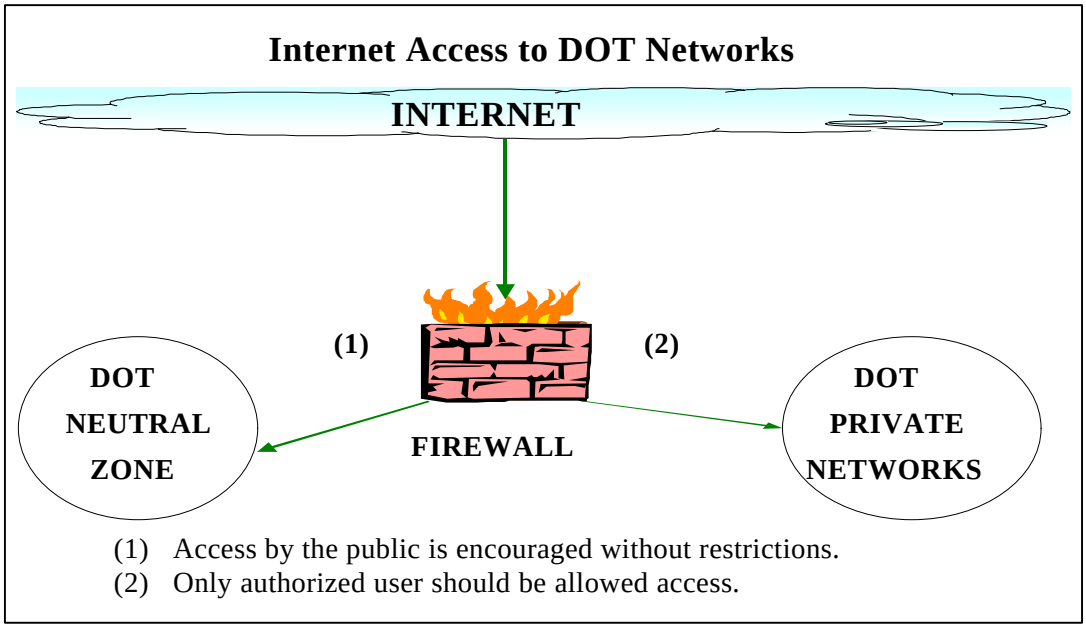
DOT Internet policy requires network services, such as HTTP web services, be disabled unless the services are needed. Although actions were taken to provide added protection to prevent unauthorized access from the Internet, we found about

900 computers located throughout DOT had active HTTP web services. Consequently, these computers were exposed to unauthorized access by insiders—another source of intrusion threat—who have a web browser on their computers. Our prior reviews identified vulnerabilities to attack and abuse by insiders. For example, we identified over 600 contractor employees, who were no longer working for DOT, still retained authorized access to DOT systems. After we identified this issue, management removed thousands of access authorizations. Our work also resulted in the prosecution of employees who embezzled funds through stolen passwords, including one who embezzled $600,000 from DOT. This security weakness occurred due to a lack of procedures to identify unneeded network services installed on DOT computers.

Public Web Servers Needed to be Separated from Private Networks

DOT's Internet policy requires that computers providing information for public viewing be maintained in a separate and secure area. DOT established a separate network area as a neutral zone to house web servers intended for public viewing. This setup was designed to prevent Internet users from getting direct access to DOT's private networks. A firewall, installed between DOT private networks and the neutral zone, acts as a "security guard" monitoring and directing network traffic into the neutral zone or DOT's private networks, as shown in Table 1.

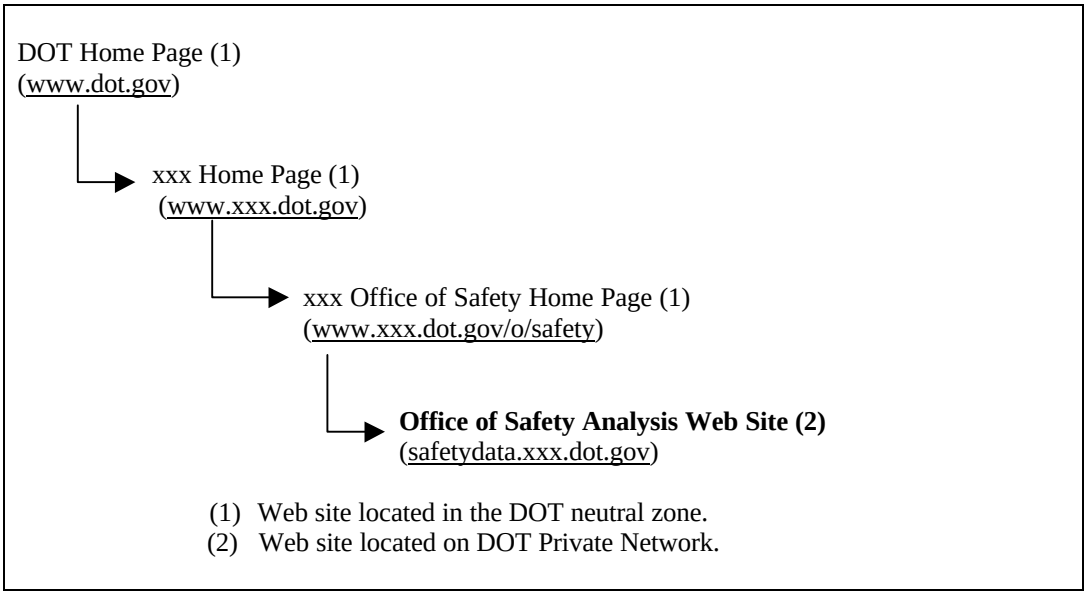
Table 1. DOT's Neutral Zone and Firewall



Our scanning of DOT servers identified 13 public web servers that were misplaced on DOT's private networks behind the firewall. Because of the misplacement, the

DOT firewall allowed Internet users to enter some of DOT's private networks. As shown in Table 2, Internet users were able to enter DOT's private networks by "clicking" on the links provided by DOT web sites.

Table 2. Unauthorized Entrance
Into DOT's Private Networks through Web Linkage



DOT's Internet policy requires computers providing information for public viewing be maintained in a separate and secure area. This weakness occurred due to DOT internal agencies' lack of awareness of DOT Internet security requirements and the adverse impact on DOT network security when public web servers are misplaced. This weakness provided opportunities to exploit computers behind the firewall on DOT private networks. As a result, intruders could:

- Attack DOT computers with tools available on hacker web sites. Such attacks could result in deleting or changing data stored on computers, stealing legitimate user names and passwords, tying up DOT computer resources (denial-of-service), or a combination of these attacks as demonstrated by the recent e-mail Love Bug virus.

- Gain privileged access to information stored on DOT computers. Once inside, intruders could use hacking tools to steal user names and passwords to masquerade as legitimate DOT users. In addition, access from within DOT computers is not subject to the same level of scrutiny as outsiders because the computer considers insiders as a "trusted source."

During the audit, we brought this matter to management's attention. As of August 3, 2000, all 13 web servers were either moved to the DOT neutral zone or

relocated outside of DOT networks, such as at contractor sites. However, enhancing security awareness training and developing procedures to detect installation of web (HTTP) services on DOT's private networks are needed to prevent recurrence.

Configuration Over Web Servers Needs to be Strengthened to Prevent Attacks

The President, recognizing the significance of recent computer attacks, issued directives to all agency heads to renew efforts to safeguard their Department or agency's computer systems against denial-of-service attacks from the Internet. On March 15, 2000, the DOT CIO issued a memorandum requiring that each DOT internal agency review the security of its web sites, and act aggressively to eliminate vulnerabilities to ensure DOT web sites are in full compliance with the DOT Internet policy.

DOT has about 240 web servers available for public access through the DOT Home Page. We scanned 119 of these web servers to determine whether they were properly configured and upgraded to reduce the risk of being defaced or disrupted. We identified a total of 111 vulnerabilities on 67 web servers in 11 DOT internal agencies. These vulnerabilities are categorized into three risk levels--41 as high, 16 as medium, and 54 as low risks. The web servers that we did not scan could have similar vulnerabilities and, therefore, need to be examined.

The three most frequently identified high vulnerabilities on DOT web servers are among the "Top Ten Internet Security Threats" issued by the Federal CIO Council. These high vulnerabilities could allow Internet users to remotely execute computer commands, such as deleting files on a web server. With such vulnerabilities, attacks on DOT's web servers could result in embarrassment (for example, web sites could be defaced), inconveniences (for example, web servers could be put temporarily out of service), or serious business disruptions (for example, reports filed by industry to meet regulatory requirements could be deleted). These negative effects could become more serious as DOT becomes more dependent on web technologies.

These vulnerabilities occurred because of weak configuration management controls over web servers. Configuration (setup) control involves making computer hardware and software arrangements that determine what the computer will do and how it will operate under such arrangements. For example, configuration control should ask/answer questions such as:

- What connections should be allowed?
- What communication tool and language should be used?
- What execution commands should be avoided?

Configuration management is the process of adding; deleting; modifying; and documenting changes to connections, addresses and commands based on changing business needs and manufacturers' advice, such as release of upgrades and fixes. DOT needs to enhance configuration management controls over web servers because:

- The three most frequent high vulnerabilities we identified could have been avoided with good configuration management controls. One of these vulnerabilities could be corrected by simply installing a security fix provided by the software manufacturer since June 1998. Fixing the other two vulnerabilities require reconfiguration of the web servers as suggested by the software manufacturers in 1996 and 1998.

- DOT does not have procedures to examine whether web servers are properly configured before their release for public use. For example, a DOT internal agency's Home Page was defaced during the audit. We found this web server was newly configured and put online without the manufacturer's latest fix being installed.

RECOMMENDATIONS

We recommend that the DOT Chief Information Officer:

1. Direct the owners of the two remaining web servers on DOT's private networks to enhance access security by encrypting user identification and passwords, or disable them.

2. Notify DOT internal agencies to disable Internet web (HTTP) services on the 900 computers we identified.

3. Develop procedures to periodically examine DOT internal agencies' computers to identify unneeded Internet services and have them disabled.

4. Enhance security awareness training to emphasize the need to place public web servers separately from DOT's private networks.

5. Require DOT internal agencies to correct the vulnerabilities we identified on the 67 web servers, and determine whether vulnerabilities exist and need to be corrected for the 121 web servers we did not scan.

6. Establish configuration management control procedures, including an independent review and approval, to ensure all web servers are adequately configured and secured before being released for use.

7. Periodically examine in-service web servers to ensure manufacturers' software fixes and upgrades are installed upon their release.

MANAGEMENT RESPONSE

A draft of this report was provided to the DOT Chief Information Officer on September 12, 2000. The Deputy Chief Information Officer responded and we considered his comments in preparing this report. The CIO Office agreed with the findings, and agreed to initiate corrective actions for Recommendations 1, 2, 3, 4, 5, and 7 by September 25, 2000, and for Recommendation 6 by January 31, 2001. The CIO Office also plans, subject to availability of resources, to offer direct "hands-on" assistance to DOT internal agencies for Recommendations 3, 6, and 7. The complete text of management comments is the Appendix to this report.

OFFICE OF INSPECTOR GENERAL COMMENTS

Actions taken and planned by the DOT Chief Information Officer are reasonable. However, issuing additional guidance and requirements to the DOT internal agencies will not ensure corrective actions are taken and that new policies and procedures are implemented. We will monitor the CIO efforts to ensure implementation of corrective actions.

We appreciate the courtesies and cooperation of DOT representatives. If you have questions concerning this report, please call Rebecca Leng or me at (202) 366-1496.

-#-

APPENDIX
(3 pages)

ACTION: Draft Report on Headquarters
Computer Network Security, DOT

Eugene K. Taylor, Jr.
Deputy Chief Information Officer, S-80

John L. Meche
Deputy Assistant Inspector General, JA-20

In response to your request, the Office of the CIO (OCIO) has reviewed the subject draft report and offers the following comments on the recommendations contained on pages 9 & 10.

1. Direct the owners of the two remaining web servers on DOT's private networks to enhance access security by encrypting user identification and passwords, or disable them.

Comment: We concur with this recommendation and will issue a memo by September 25, 2000 directing this action to be taken within two weeks and that the system owners report back to OCIO when they have completed their work.

2. Notify DOT internal agencies to disable Internet web (HTTP) services on the 900 computers we identified.

Comment: We concur with this recommendation and will issue a memo (by September 25, 2000) directing the OAs to evaluate these computers within thirty days to determine if having HTTP services activated is necessary, and, if not, to disable service. We will also ask that the OAs report back to OCIO once they have completed this effort.

3. Develop procedures to periodically examine DOT internal agencies' computers to identify unneeded Internet services and have them disabled.

Comment: We concur with this recommendation and will issue a memo (by September 25, 2000) directing the OAs to periodically evaluate their computers and disable unneeded services. We will recommend that they examine their systems at least every 90 days and more frequently if events warrant (e.g. new type of vulnerability is identified that impacts their server's operating system). In the future

(subject to availability of resources), the OCIO plans to develop an intranet site to provide system owners with links to websites where they can obtain configuration information for their systems, and to offer direct "hands-on" assistance in the configuration of systems.

4. Enhance security awareness training to emphasize the need to place public web servers separately from DOT's private networks.

Comment: While we agree with the intent of the recommendation, the OCIO does not view this as an awareness training issue, since awareness training normally is more general in nature. Current policy exists prohibiting publicly accessible web servers from residing on the DOT internal network. With the exception of the two web servers identified in recommendation #1, all other DOT web servers are located either in the DMZ or at contractor facilities. We will reiterate this policy as part of the previously mentioned memo to ensure that it is applied to all new servers.

5. Require DOT internal agencies to correct the vulnerabilities we identified on the 67 web servers, and determine whether vulnerabilities exist and need to be corrected for the 121 web servers we did not scan.

Comment: We concur with this recommendation. CIOs were notified at the CIO Council meeting on September 20, 2000 that they must correct the vulnerabilities already identified by September 22, 2000, or disable the server. We will issue a memo (by September 25, 2000) confirming this direction and directing the OAs to evaluate remaining servers and correct any discovered vulnerabilities within sixty days. We will ask that the OAs report back to OCIO once they have completed this effort.

6. Establish configuration management control procedures, including an independent review and approval, to ensure all web servers are adequately configured and secured before being released for use.

Comment: We concur with this recommendation. OCIO will develop a "checklist" (within 120 days) that the OAs can use to perform a self-certification of their servers prior to their use. The certification will require concurrence by someone in the system owner's management chain (i.e., one or more levels above the system owner) before the system is placed in service. In the future (subject to availability of resources), the OCIO plans to develop an intranet site to provide detailed information on the self-certification process, and to offer direct "hands-on" assistance in the completion of the "checklist".

7. Periodically examine in-service web servers to ensure manufacturers' software fixes and upgrades are installed upon their release.

Comment: We agree with the intent of the recommendation, but do not fully concur with the recommended solution. It is not always advisable to immediately install vendor patches until you have determined what impact the patch might have on your system. We will include in the September 25 memo the requirement that OAs ensure that System Administrators and IT Security personnel track the release of all patches and updates so that they can quickly evaluate the need for a patch to correct a vulnerability, determine any problems the patch might cause, and if no problems are detected install required patches within 30 days of their release. In the future (subject to availability of resources), the OCIO plans to develop an intranet site to provide system owners with links to vendor sites where they can obtain the latest patches, and to offer direct "hands-on" assistance in the setup or inspection of systems.