Before the Committee on Science

U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EDT
Wednesday
September 27, 2000
Report Number: CC-2000-359

Computer Security Within the U.S. Department of Transportation

Statement of

The Honorable Kenneth M. Mead

Inspector General

U.S. Department of Transportation

Mr. Chairman, Ranking Member Hall, and Other Members of the Committee:

We appreciate the opportunity to testify today on computer security issues within the Federal Aviation Administration (FAA) and the Department of Transportation (DOT). Computer security is getting increased attention due to Presidential Decision Directive 63, which calls for protecting the nation's critical infrastructure by May 2003. That will be a challenge for DOT because, as we previously reported, computer security is one of the top management issues facing DOT.

DOT, with $2.7 billion in planned expenditures in Fiscal Year 2000, is responsible for the largest information technology investment of all Federal civilian agencies. About 80 percent of planned expenditures are for FAA. DOT has over 600 mission-critical systems, including safety-sensitive air traffic control systems, Coast Guard search and rescue systems, and financial systems supporting the accounting for, and distribution of, billions of dollars in Federal funds. Most Internet users have no need to access, and should not be allowed access to, computers in DOT's private networks. Our testimony will address these areas:

- The need to strengthen personnel security for DOT employees and contractor personnel authorized to access DOT systems,
- The need to strengthen network security to prevent unauthorized access by Internet users or insiders. Our prior reviews have resulted in criminal prosecution of abusive insiders, and
- The need to strengthen web security to ensure integrity of DOT E-Government business.

First, a survey performed by the Federal Bureau of Investigation in 1998 reported that insiders constitute the greatest intruder threat. With this in mind, both DOT and FAA need to improve personnel security over Government employees and contractor personnel with authorized access to DOT computer systems.

DOT's personnel security policy requires different levels of background checks on employees based on designated position sensitivity level. Background checks provide valuable information, but by no means provide guarantees as to a person's loyalty or trustworthiness. DOT employees and contractor personnel performing comparable duties should have the same kind of background checks, but they do not. Without proper background checks, DOT could be missing valuable information that might keep some contractor personnel who are at risk from working on certain DOT contracts. This is especially important to FAA in view of the billions of dollars of work done by contractor personnel to develop and

maintain program code for FAA's air traffic control National Airspace System (NAS).

In December 1999, the General Accounting Office (GAO) reported that FAA did not conduct background checks on foreign national contractor personnel performing Year-2000 renovation work on FAA's mission-critical systems. FAA agreed to bring its many contracts into compliance with the personnel security policy. In June, we recommended that FAA upgrade background checks on contractor personnel.

On June 30, 2000, FAA agreed to upgrade the level of background checks on contractor personnel working on air traffic control systems. On September 22, 2000, FAA reported that background checks are required on 3,041 contractors working on its mission-critical systems, of which 1,975 have been completed. However, background checks on the majority of these contractors need to be upgraded beyond fingerprint checks. A full plan for completing all background checks is not in place. FAA needs to work with the Office of Personnel Management (OPM) to develop a workable plan with firm milestones to complete background checks on contractor personnel.

We recently completed a review of a DOT financial system and 13 headquarters computer network systems throughout DOT. These audits generally identified the lack of background checks on contractor personnel, including foreign nationals, throughout DOT and the appropriate level background checks generally were not made on DOT employees. We also found some contractor personnel, who received no background checks, were tasked to perform sensitive work such as managing DOT's network security. DOT agreed to have these background checks completed within 6 to 12 months.

Second, DOT relies on network security software—firewalls—to direct network traffic into either DOT's private networks or to public web sites. This is an important control in today's highly interconnected network environment. We identified weaknesses in DOT's network security that made DOT computers vulnerable to attack from outside of and within DOT.

Internet Access: By logging on as an Internet user, we gained access from the Internet to about 270 computers located within DOT's private networks. These computers were located throughout DOT; however none was found at FAA Headquarters. We also found 13 web sites (none in FAA) intended for public access were inappropriately placed on DOT's private networks. As a result, DOT's firewalls allowed Internet users to enter DOT's private networks. When we brought this to management's attention, Internet access security was strengthened. DOT must improve firewall security, enforce access security requirements, and

increase employees' security awareness training to prevent these problems in the future.

For FAA, the challenge to secure Internet access is different. The current computer networks supporting NAS operations are relatively immune from intruders because of the system's physical isolation. However, as part of its NAS modernization, FAA is considering replacement of these physically isolated networks with an integrated network supporting both administrative and NAS operational needs.

Replacing what are now separate networks with an integrated network could lead to additional exposure for the NAS because the integrated network will have connections to the Internet. This change will require FAA to install sophisticated network access controls, and examine whether air traffic control systems connected to the integrated network require security upgrades. Until the NAS vulnerability is fully assessed and FAA can give assurances that the common network approach will not compromise NAS security, FAA should not proceed to integrate the NAS and administrative systems on a common network.

Insider Access: We found about 900 computers located throughout DOT were vulnerable to attack by insiders, such as employees or contractors. These computers have web services (HyperText Transfer Protocol--HTTP) installed, which made them easy to access. This is an important concern to DOT in view of the large number of contractors (estimated 40,000) working on DOT systems. Our prior reviews identified vulnerabilities to attack and abuse by insiders. For example, we identified over 600 contractor personnel, who were no longer working for DOT, still retained authorized access to DOT systems. 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 web services on these computers.

Third, DOT has about 240 web servers for public access through its Home Page. Of the 119 web servers reviewed, we identified 111 vulnerabilities, some of which were rated as high risks. Attacks on web sites could range from mere embarrassment (web sites defaced), to inconveniences (web servers out-of-service), or serious business disruptions (deleting reports filed by industry to meet regulatory requirements). DOT management has taken corrective actions and is strengthening configuration management controls over web servers.

We also found 22 of DOT's web sites, which were connected to its Home Page, used "Cookies"—a mechanism used by web sites to collect information about visitors. While no user-identifiable information was collected, these sites

collected information such as which document is downloaded most frequently. However, in doing so, DOT did not post clear notices advising visitors of "Cookies" usage. Also, half of these web sites did not disclose how the collected information was used, as required by DOT policy. When we brought this to management's attention, use of "Cookies" at nine web sites was disabled. Management agreed to enhance the notice and disclosure for the remaining web sites.

Presidential Decision Directive 63 requires upgrading and enhancing security across the Federal Government. This is a long-term and expensive effort for the Federal Government and certainly for DOT. While fixing computer security weaknesses is technically different from Year-2000 problems, there are many similarities from a methodological and management perspective. Like Year-2000 work, risk assessments and decisions on the level of computer security must be made, priorities established, milestones set, money and staff obtained, and top level management committed to get the job done.

BACKGROUND

We have been reviewing DOT's network security since 1997 when we found DOT lacked firewalls to prevent Internet users from navigating DOT's private networks or using DOT networks to gain access to other computers. Since then, DOT installed firewalls to secure entry points from the Internet.

In May 1998, the President issued a white paper on Critical Infrastructure Protection (Presidential Decision Directive 63) that required the Nation's critical infrastructure, both physical and cyber-based, be protected from intentional destructive acts by May 2003. In March 2000, the President also issued an action memorandum that required Federal agencies to safeguard computer systems against denial-of-service attacks from the Internet.

In our December 1999 report to the Secretary and Congress, we identified computer security as one of the top management issues facing DOT. The recent experience with Year-2000 computer problems pointed out how much our

business and personal lives depend on interconnected computer systems. Recent high profile hacker attacks on major companies' computer systems and the spread of the e-mail Love Bug virus demonstrate that computers are vulnerable to attacks in today's interconnected network environment.

ACCESS TO DOT COMPUTER SYSTEMS

DOT, with $2.7 billion in planned expenditures for Fiscal Year 2000, is responsible for the largest information technology (IT) investment among all Federal civilian agencies. FAA accounts for about 80 percent of these planned IT expenditures. DOT has over 600 mission-critical systems, including safety-sensitive air traffic control systems, Coast Guard search and rescue systems, and financial systems supporting the accounting for, and distribution of, billions of dollars in Federal funds. These computer systems operate on DOT's private networks, which are supposed to be restricted to authorized users.

DOT also has over 240 web sites connected to the DOT Home Page that it encourages the public to access from the Internet. DOT uses these web sites to comply with the Paperwork Reduction Act requirements--disseminating information such as regulations timely, and minimizing the paperwork burden when collecting information, such as surveys of the transportation industry. These web sites are placed in public viewing areas. While DOT encourages use of its public web sites, most Internet users have no need to access, and should not be allowed access to, computers in DOT's private networks.

CONTROLS OVER AUTHORIZED USERS' ACCESS

Thousands of people are authorized to access DOT computer systems on its private networks, including DOT employees, grantees, contractor personnel, and other Government agencies. These users are authorized to perform various functions such as developing or maintaining hardware or software, writing computer code, updating computer information, reviewing information within computer systems, and keeping some systems in operation 365 days a year.

A survey performed by the Federal Bureau of Investigation in 1998 reported that insiders constitute the greatest intruder threat. Prior Office of Inspector General (OIG) reviews also identified vulnerabilities to attack and abuse by insiders. To ensure integrity, confidentiality, and availability of computer operations, adequate personnel controls have to be established in conjunction with management controls (control policies and procedures); operational controls (physical security, contingency planning); and technical controls (access security, network intrusion/detection).

Common personnel control techniques include segregating key duties among staff, holding individuals accountable for actions, restricting individuals' access to the minimum necessary for job performance and conducting proper background checks on individuals in positions of trust. This part of our testimony focuses on background checks for authorized users.

DOT's personnel security policy[1] includes four different levels of background checks on employees, based on designated position sensitivity level or risk level. The policy provides specific guidance on computer-related positions. Most

[1] DOT Order 1630.2A, entitled "Department of Transportation Personnel Security Handbook."

computer-related positions would be categorized as either critical sensitive/high risk (with more extensive background checks) or non-critical sensitive/moderate risk (with lower level background checks). DOT policy also requires the same type of background checks on contractor personnel that perform comparable duties to DOT employees.

Background checks provide valuable information, but by no means provide guarantees as to a person's loyalty or trustworthiness. Table 1 summarizes position designation and background check requirements specified in DOT policy.

Table 1

Position Designation	**Type of Minimum Background Checks Required**	**Tasks Included**
Special Sensitive	Single Scope Background Investigation (SSBI)	➢ Personal interviews (with at least 7 years coverage) ➢ $2,600 to $3,000 in costs ➢ 6 to 9 months to complete ➢ Updates every 5 years
Critical Sensitive/ High Risk	Background Investigation (BI)	➢ Personal interviews (with 5 years coverage) ➢ $2,300 to $2,700 in costs ➢ 3 to 12 months to complete ➢ Updates every 5 years
Non-critical Sensitive/ Moderate Risk	National Agency Check And Inquiry (NACI)	➢ Documentation review only ➢ $77 in costs ➢ 4 to 6 months to complete ➢ No updates
Non-sensitive/ Low Risk	NACI (for DOT employees) Fingerprint check (for contractor personnel)	NACI check (see above) Fingerprint check includes: ➢ Checks against FBI criminal records ➢ $18 to $28 in costs

Background Checks on FAA Authorized Users

In a December 1999 report, GAO reported that FAA did not conduct background checks on foreign national contractor personnel performing Year-2000 renovation work on FAA's mission-critical systems. FAA agreed to review whether background checks have been conducted on all contractor personnel, including foreign nationals. FAA reported that it is working to bring its many contracts into compliance with the personnel security policy.

Having proper background checks on contractor personnel is important to FAA. Multi-billions of dollars of work is done by FAA contractor personnel on systems critical to the safety and stability of the NAS, such as writing, repairing, and testing of computer code. For example, contractor personnel work on software-intensive systems such as the Wide Area Augmentation System (WAAS)—a navigation system using the Global Positioning Satellite System technology, and the Standard Terminal Automation Replacement System (STARS)—a commercial based, fully digital system supporting air traffic control operations at major air traffic facilities. Without proper background checks, FAA could be missing valuable information that might keep some contractor personnel who are at risk from doing this work.

Since April 2000, FAA has taken action in its new contracts to require background checks on contractor personnel. FAA reported 343 (out of a total of 435) mission-critical systems do not require any additional security assessment because the contracts are closed, or the contracts do not involve personnel support, such as software purchase contracts. For the remaining 92 systems, FAA has initiated (requested) background checks on contractor personnel for all but 7 systems. FAA plans to complete risk assessment and background check initiation on these 7 systems by September 30, 2000.

FAA originally concluded about 90 percent of these contractor personnel positions were of low risk and required only fingerprint checks. In June, we recommended that FAA upgrade the requirement because of the sensitivity of air traffic control systems. On June 30, 2000, FAA agreed to upgrade the minimum level of background checks to NACI for contractor personnel working on air traffic control systems.

On September 22, 2000, FAA reported that background checks are required on 3,041 contractors working on its mission-critical systems, of which 1,975 have received background checks—48 received extensive checks, 545 received lower level background checks, and the remaining 1,382 contractors received fingerprint checks only (see Table 2). FAA estimates that background checks on the majority of these 1,382 contractors need to be upgraded. FAA expects background checks to be completed in 8 to 10 weeks after the requests are initiated; but no target dates have been established for completing all background checks.

Table 2

Background Check Types	**Requested**	**Completed**
OPM-- Background Investigation (BI)	65	48
NACI	1,068	545
Fingerprint Check	1,552	1,382
In Process	140	0
Processed by Other Agencies	216	N/A
Totals	-------- 3,041 ====	------- 1,975 ====

While FAA has made progress in this area, much remains to be done. Because this is a sizable task, FAA needs to work with OPM to develop a workable plan with firm milestones to complete background checks on contractor personnel. A full plan is still not in place. As indicated in Table 1 on page 7, DOT's experience with background checks has been 4 to 6 months to complete a lower level check

(NACI) and 3 to 12 months to complete the higher level check (BI). It will be some time before all the required background checks are completed on contractor personnel, and even more time to take management actions such as removal of personnel from contracts, if warranted.

Background Checks on Other DOT Authorized Users

OIG recently completed a review of a DOT financial system supporting the Federal Transit Administration and 13 headquarters computer network systems supporting all DOT Operating Administrations. It is clear that FAA is not alone in facing the challenges of computer security. These reviews found background checks generally were not conducted on contractor personnel throughout DOT, and the appropriate level of background checks generally was not made on DOT employees. According to DOT policy, key DOT and contractor personnel authorized to access these DOT computer systems should receive more extensive BI background checks while others should receive lower-level NACI background checks.

- Financial Management System: A total of 34 DOT employees and contractor personnel, including 3 foreign nationals, are responsible for maintaining, modifying, and securing this Federal Transit Administration financial system, which is used to manage and account for billions of dollars. For this financial system, contractor personnel had access to both the program source codes and data files. DOT had not conducted the more extensive background checks on any of its employees, and no background checks at all were done on contractor personnel. The contract did not include language requiring background checks

on contractor personnel[2]. Management agreed to take appropriate actions to meet DOT's personnel security requirements by June 2001.

- Headquarters Network Systems: A total of 102 DOT employees and contractor personnel, including 2 foreign nationals, are responsible for maintaining, modifying, and securing 13 headquarters computer network systems supporting all DOT Operating Administrations. These computer networks store sensitive data and transmit transactions, such as grant approvals, contract payments, and payroll changes. According to DOT policy, at least one position for each of these 13 network systems should have been designated as high risk, and employees in those positions should receive more extensive BI background checks. Of the 41 DOT employees, OIG found a total of 4 in FAA, Coast Guard, and the Office of the Secretary were designated as occupying high-risk positions and received corresponding BI background checks. For the remaining 37 employees, 33 received at least the NACI background checks. Four employees did not receive any background checks. In September 2000, DOT agreed to have appropriate employee background checks completed in 6 to 12 months.

  For the 61 contractor personnel, we found a wide range in levels of background checks. One Coast Guard contractor personnel received extensive BI background checks. Five FAA contractor personnel received fingerprint checks to obtain building entrance passes. Other contractor personnel received no background checks at all. Some of these contractor personnel are tasked to perform sensitive functions such as managing DOT's network security, for which fingerprint checks would not be sufficient. Further, requirements for

[2] OIG Report entitled "Computer Security Controls of Financial Management System--Federal Transit Administration," May 23, 2000 (Report Number: FE-2000-098).

background checks were not consistently included in DOT contracts. DOT agreed to correct these problems within 12 months[3].

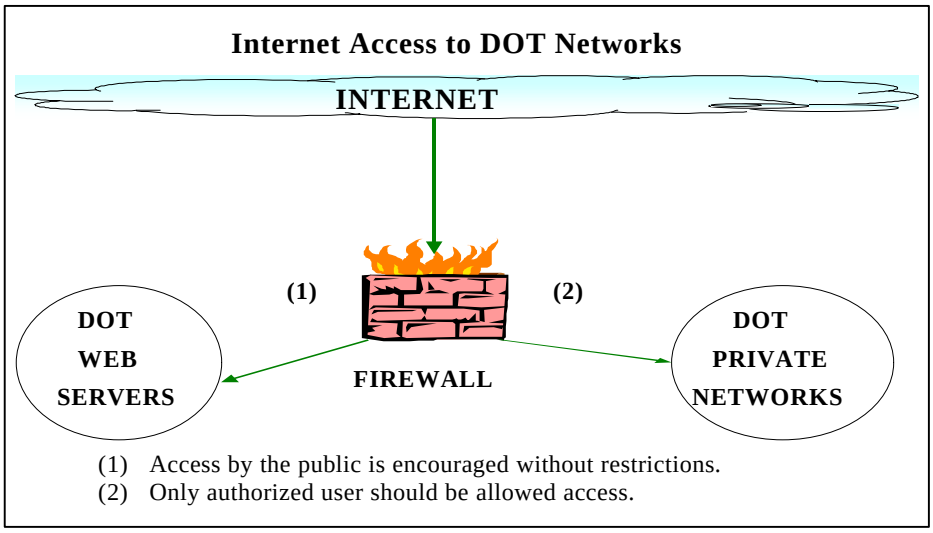
Without the proper level of background checks, management could be missing valuable information about people who are placed in key positions to ensure the integrity and security of computer system operations. DOT needs to enhance management awareness of personnel security agencywide, include appropriate language in computer contracts that a certain level or levels of background checks must be completed on contractor personnel, and must have contracting officers enforce compliance.

CONTROLS OVER UNAUTHORIZED USERS' ACCESS

Access to DOT Networks

DOT relies on network security software—firewalls—to direct network traffic from the Internet into either DOT's private networks or to public viewing sites as shown in Table 3.

Table 3



[3] OIG Report entitled "Interim Report on Computer Security," July 13, 2000 (Report Number: FI-2000-108).

Because DOT's computer networks are highly interconnected, it is extremely important that only authorized users are granted access. Our audits have identified weaknesses making DOT's networks vulnerable to both outsiders (such as Internet users) and insiders (such as employees, contractor personnel, or grantees):

- 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 found at FAA or U.S. Coast Guard Headquarters. After we brought this to management's attention, DOT network security was strengthened to eliminate this vulnerability.
- While most of DOT web sites intended for public viewing were placed in the separate public viewing area, we found 13 of them were inappropriately placed on DOT's private networks. As a result, DOT's firewalls allowed Internet users to enter DOT's private networks. However, none of the 13 sites belong to FAA or Coast Guard. When we brought this to management's attention, these web sites were removed from DOT's private networks.
- About 900 computers located throughout DOT have unneeded web services (HTTP) installed, and accordingly are accessible on DOT's private network. Any computer user equipped with a web browser, which is becoming a standard feature on personal computers, can access these machines. As a result, they were vulnerable to attack by insiders; such as disgruntled employees or contractor personnel. This is an important concern to DOT in view of the large number of contractor personnel (estimated 40,000) working on DOT systems. DOT management agreed to disable unneeded network services on these computers.

Also, our prior reviews identified vulnerabilities to attack and abuse by insiders. For example, we identified over 600 former DOT contractor personnel who still retained authorized access to DOT systems. After we brought this issue to management's attention, they removed thousands of access authorizations. Our work also resulted in the prosecution of employees who embezzled funds by using stolen passwords, including one former employee who embezzled $600,000 from DOT.

Getting inside DOT's private networks gives unauthorized Internet users an opportunity to exploit weaknesses on DOT computers. Once inside, intruders could launch various attacks resulting in deleting or changing data, stealing user names and passwords, tying up computer resources (denial-of-service), or a combination of these as demonstrated by the recent e-mail Love Bug virus.

Equally important, once inside the private network, the computer system recognizes all users as "authorized to be there," which could allow intruders to masquerade as legitimate DOT users to access information stored on DOT computers. Since many of DOT's networks are connected with each another, a control weakness in one part of a network could compromise the rest of DOT's networks.

DOT needs to improve firewall security, increase employees' security awareness training, and develop procedures to identify and disable unneeded network services on its computers to prevent recurrences of these problems[4].

[4] The OIG Report entitled "Headquarters Computer Network Security," September 25, 2000 (Report Number: FI-2000-124) focused on headquarters computer network operations within DOT. Network security over FAA and Coast Guard field operations will be covered in future audits.

Access to FAA's National Airspace System

As reported by the President's Commission on Critical Infrastructure Protection[5], the current networks supporting the NAS operations are relatively immune from intruders because of the system's physical isolation. Currently, the NAS is not connected to administrative networks, so there is no need to worry about interconnections with administrative computer systems.

In August 1998, we testified before the House Subcommittee on Technology that FAA, as part of its NAS modernization, was planning to use a common network to support both administrative and NAS operational needs. Through our ongoing FAA Telecommunications Infrastructure (FTI) review, we found that FAA is currently considering replacement of its isolated network with an integrated network.

Replacing what are now separate networks with an integrated network could lead to additional exposure for the NAS because the integrated network will have connections to the Internet to support FAA administrative functions. This change will require FAA to install sophisticated network access controls and enhance security in the existing and future air traffic control systems connected to the integrated network.

Currently, FAA is conducting vulnerability assessments of its 102 air traffic control systems, which were deemed essential to the Nation's critical infrastructure. FAA has completed assessments for 44 systems, but system

[5] As a result of this Commission's report, the President issued Presidential Decision Directive 63 that requires the Nation's critical infrastructure, both physical and cyber-based, be protected from intentional destructive acts by May 2003. DOT submitted its Critical Infrastructure Protection Plan to the National Security Council in August 1999.

assessments for all the remaining systems will not be completed until December 2001. Without complete assessments, FAA cannot estimate the time and resources needed to enhance NAS security. Until the NAS vulnerability is fully assessed and FAA can give assurances that the common network approach will not compromise NAS security, FAA should not go forward to integrate the NAS and administrative systems on a common network as part of the FTI project.

CONTROLS OVER WEB SECURITY

Vulnerabilities to Attack

DOT has about 240 web servers available for public access through the DOT Home Page. We reviewed 119 of these servers and identified a total of 111 vulnerabilities on 67 web servers. These vulnerabilities are categorized into three risk levels—41 as high, 16 as medium, and 54 as low risks[6]. The three most frequently identified high vulnerabilities on DOT web servers are among the "The Ten Most Critical 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 web servers could result in embarrassment (web sites defaced), inconveniences (web servers out-of-service), or serious business disruption (reports filed by industry to meet regulatory requirements deleted). These negative effects could become more serious as DOT becomes more dependent on web technologies to meet the Government Paperwork Elimination Act

[6] 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.

requirements. The Act requires Government agencies to provide for the option of electronic maintenance, submission, or disclosure of information as a substitute for paper by October 2003.

These vulnerabilities occurred because of weak controls over web configuration (computer setup). For example, one of the three most frequent high vulnerabilities could be corrected by installing a security fix provided by the software manufacturer since 1998. Fixing the other two vulnerabilities requires reconfiguration of the web servers as suggested by the software manufacturers in 1996 and 1998. DOT has taken corrective actions on these vulnerabilities and agreed to develop a checklist, by January 2001, for certifying web servers prior to release for use.

Use of "Cookies"

OIG found that 22 of DOT's public web sites used "Cookies" to collect information from the public. "Cookies," an Internet mechanism, lets web sites collect information from visitors. DOT policy prohibits using "Cookies" to collect user-identifying information such as previously visited sites, e-mail addresses, or other information to build profiles on individual visitors. When used in legitimate cases, DOT policy requires clear and conspicuous notices advising visitors of the "Cookies" usage, and appropriate disclosure of how the information collected is handled.

While the 22 DOT sites did not collect user-identifiable information, they collected information such as which document is downloaded most frequently. However, in doing so, DOT did not post clear and conspicuous notices of "Cookies" usage. Also, half of these sites did not disclose how the collected information is used. After we brought this issue to management attention, use of

"Cookies" at nine sites was disabled. DOT agreed to enhance notices and disclosure for the remaining sites.

We have an ongoing review of FAA Telecommunication Infrastructure and plan to issue a separate report with recommendations for improving computer security at FAA. We will continue to monitor computer security issues throughout DOT in our future work, and advise Departmental officials and Congress of progress and problems.

Mr. Chairman, Ranking Member Hall, this concludes our statement. I would be pleased to answer questions.