7. COMPUTER SECURITY

DOT must aggressively address known risks and also take on the challenge of identifying and addressing the unknown risks associated with computer security in today's interconnected world. A 1997 study by the President's Commission on Critical Infrastructure Protection pointed out widespread capability to exploit the Nation's infrastructure vulnerabilities, particularly through information networks.

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. The most important of the President's initiatives in this area is Presidential Decision Directive 63 (PDD-63) which requires that the Nation's critical infrastructure, both physical and cyber-based, be protected from intentional destructive acts.

In addition to managing unauthorized access or attacks by outsiders, agencies also need to enhance security over insiders, including employees, contractors, and grantees. A survey performed by the Federal Bureau of Investigation (FBI) reported that insiders constitute the greatest intruder threat. In DOT, two employees were recently prosecuted for embezzling funds through stolen passwords, including one who embezzled $600,000 from DOT.

E-Government is becoming an important part of Government operations. Web sites are powerful tools for the Federal Government to improve the quality of its services. However, until people are confident that their privacy is protected, they will not use the services provided on Government sites.

Progress in the Last Year:

- DOT identified 108 information systems as critical to the Nation's infrastructure. DOT is developing schedules to complete assessment of these systems' vulnerabilities by September 2001 and allocating resources to have these systems secured by May 2003, as required by PDD-63.

- DOT enhanced network firewall security to prevent unauthorized Internet access to DOT's private networks as a result of OIG findings.

- DOT established Computer Security Incident Response Capabilities to detect and prevent malicious activities. For example, FAA has installed 12 network intrusion detection mechanisms to protect its private networks. Also, DOT plans to ask FAA to lead the coordination with the FBI National Infrastructure Protection Center, which is the national focal point for gathering information on threats to critical infrastructures.

- DOT started providing information security awareness training to employees. FAA completed this task by providing training videotapes to all its employees.

- DOT examined the validity of 73,000 user accounts authorized to access DOT systems and removed over 5,000 access authorizations.

Most Significant Open Recommendations and Issues:

- Completing the Vulnerability Assessments of Infrastructure Mission-critical Systems. This is important to help determine resource needs and prioritize which computer vulnerabilities to fix first. DOT deemed 108 systems essential to the Nation's economy and security, which need to be secured against intentional attacks by May 2003, as required by PDD-63. These include 102 FAA systems supporting air traffic control operations and 6 U.S. Coast Guard systems supporting search and rescue and maritime safety operations. While the Coast Guard has completed the vulnerability assessment, FAA still is assessing vulnerabilities associated with its air traffic control systems. FAA plans to complete all assessments by September 2001. Without complete assessments, FAA cannot estimate the time and resources needed to secure these systems and prioritize the vulnerabilities that need to be fixed first.

- Evaluating the Security Impact of the Proposed Integration of the National Airspace System for Air Traffic Control and FAA Administrative Systems. The current computer networks supporting National Airspace System (NAS) operations are relatively immune from intruders because of the system's physical isolation. However, 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 requires determining that the common network approach will not compromise NAS security because the integrated network will have connections to the Internet. 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 air traffic control and administrative systems on a common network.

- Completing Proper Background Checks on DOT Employees and Contractor Personnel, and Incorporating Background Check Requirements in Contracts. DOT policy requires background checks on both employees and contractor personnel based on designated position sensitivity level or risk level. OIG found a lack of proper background checks on contractor personnel and DOT employees tasked to maintain and secure Headquarters network systems, which were critical to DOT operations. For 102 DOT employees and contractor personnel reviewed, only 4 DOT employees and 1 contractor employee received extensive background checks. Fifty-five (55) contractor personnel did not receive any background checks. FAA is in the process of identifying all contractor personnel associated with its air traffic control systems for background checks and requiring more comprehensive background checks for thousands of contractor personnel.

- Implementing Security Measures against Attacks on DOT Computers and Improving Controls over Passwords. OIG found DOT computers were accessible by unauthorized Internet users. Specifically, OIG gained unauthorized access from the Internet to about 270 computers located within DOT's private networks. Also, Internet users were able to bypass DOT's firewall security and gain access to DOT's private networks because 13 public web servers were inappropriately placed on DOT's private networks. As a result of OIG audits, DOT has enhanced firewall security against unauthorized Internet access and removed public web servers from DOT's private networks. OIG also found that 900 computers located throughout DOT could be accessed by unauthorized insiders such as employees, contractors, and grantees. OIG's prior reviews identified other vulnerabilities to attack and abuse by insiders. For example, our work resulted in the prosecution of two employees who embezzled funds through stolen passwords, including one who embezzled $600,000 from DOT.

- Ensuring that Third-party Networks (such as Contractors, Trade Associations, or State Agencies) Connected to DOT Systems are Secured. Third-party connections provide another avenue for non-DOT personnel to gain access to DOT's private networks. However, access through these connections is not subject to firewall security controls. Instead, DOT's policy is to obtain "Statements of Conformance" from these third parties certifying that their computer systems are in compliance with DOT security requirements. OIG found conformance statements were not being obtained.

- Completing Certification and Accreditation of DOT Systems. Both the Office of Management and Budget (OMB) and DOT require that management assess whether controls and security in computer systems are commensurate with the risk resulting from the loss, misuse, unauthorized access to, or modification of, the computer systems. OIG found a mission-critical DOT financial management system, which was used to manage billions of dollars, was placed into operation without certification and accreditation. OIG was able to gain unauthorized access to the system's primary computer by using a widely known user identification "code."

- Eliminating Vulnerabilities on Web Servers and Developing a "Checklist" to Help Ensure Proper Configuration of Web Servers. DOT has over 240 web servers that it encourages the public to access from the Internet through the DOT Home Page. Of the 119 web servers reviewed, OIG identified a total of 111 vulnerabilities that made DOT web sites susceptible to attack. Such attacks could result in web sites being defaced or web servers being put out-of-service.

- Ensuring Proper Use of Cookies on DOT Web Sites. The term "cookie" represents a mechanism used on web sites to collect information by placing small bits of software on web users' computers. There are two types of cookies—persistent cookies and session cookies. Session cookies are used only during a single browsing session and do not collect information in ways that raise privacy concerns. Conversely, persistent cookies track information over time or across web sites. They remain stored on visitor computers until the specified expiration date, and can be used to collect individual browsing information, such as the visitor's areas of interest. Use of persistent cookies on DOT web sites requires the Secretary's approval and disclosure of the use of cookies.

  OIG first reported improper use of cookies on DOT's web sites in August 2000. A followup review in October disclosed a lack of progress including use of persistent cookies without the Secretary's approval and thousands of web pages not checked for potential use of cookies. As of December 2000, all DOT components, except FAA, have certified their use of cookies to be in compliance with DOT policy. OIG's independent testing validated the certification; however, the testing still detected use of unauthorized cookies on FAA web sites. FAA has agreed to check all web pages for corrections by January 31, 2001.

Key OIG Contact: John L. Meche, Deputy Assistant Inspector General for Financial, Information Technology, and Departmentwide Programs, 202-366-1496.

7. Computer Security

Dark Grey = Top Priority Task for 2001

Light Grey = Include in 2001 Top Management Challenges Efforts

White = Sufficiently Resolved to be Dropped from Management Challenges Efforts

	First Year Issue Raised in OIG Management Challenges Report	Was Significant Progress made in last year?
• Ensure that third-party networks connected to DOT systems are secured.	1998	N
• Complete proper background checks on DOT and contractor employees, and incorporate background check requirements in all existing and new system contracts.	New Issue	New Issue
• Implement security measures against attacks and improve controls over passwords.	New Issue	New Issue
• Complete certification and accreditation of DOT systems.	New Issue	New Issue
• Eliminate vulnerabilities on web servers and develop a “checklist” to help ensure proper configuration of web servers.	New Issue	New Issue
• Ensure proper use of cookies on DOT web sites.	New Issue	New Issue
• Identify and cancel all system user accounts assigned to contractor and DOT employees who no longer work for DOT.	1998	Y
• Require all system user accounts in the security database to be validated, and develop a policy for re-validation of employees and contractors.	1998	Y