Information Security Program

Department of Transportation

Report Number: FI-2001-090
Date Issued: September 7, 2001

Memorandum

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

Subject: **ACTION**: Report on Information Security Program, DOT
FI-2001-090

Date: September 7, 2001

Reply To
Attn Of: Meche: x61496

From: Alexis M. Stefani
Assistant Inspector General for Auditing

To: Deputy Chief Information Officer

INTRODUCTION

This report presents the results of the Office of Inspector General (OIG) audit of the information security program at the Department of Transportation (DOT). Our audit objective was to satisfy the legislative mandate of the Government Information Security Reform Act (GISRA) which requires an annual independent evaluation of agencies' information security programs. In addition to this report, we provided input (Exhibit A) to DOT's GISRA Executive Summary by answering 12 questions specified by the Office of Management and Budget (OMB).

GISRA requires Federal agencies to identify and provide security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, information collected or maintained by or on behalf of an agency. DOT, with $2.7 billion in planned expenditures in FY 2002, is responsible for one of the largest information technology investments of all Federal civilian agencies. About 80 percent of planned expenditures are for the Federal Aviation Administration (FAA).

DOT has about 1,200 computer 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. The air traffic control and search and rescue systems support Federal programs deemed by OMB to have a high impact on the public. These systems operate on DOT's private computer networks that should be accessed only by authorized personnel. DOT also has more than 150,000 web pages accessible to the public through the Internet.

Information security also is the focus of Presidential Decision Directive (PDD) 63, which calls for protecting the Nation's critical infrastructure, both cyber and physical, by May 2003. In 1998, DOT identified the systems and facilities used to support air traffic control, U.S. Coast Guard search and rescue, and marine safety operation; as well as the Saint Lawrence Seaway as PDD-63 critical assets.

For this audit, we also included results from 20 General Accounting Office (GAO) and OIG audit reports and 5 testimonies on DOT computer security for about 3 years as of September 7, 2001 (Exhibit B).

RESULTS IN BRIEF

While GISRA addresses similar security provisions as specified in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996, it also emphasizes the need for enhanced computer security in today's inter-connected network environment. Beginning in Fiscal Year (FY) 2000, we reported computer security as one of the top management challenges facing DOT because of the increased network exposure and vulnerabilities we previously identified.[1]

In the last 3 years, we made numerous recommendations to correct deficiencies and reduce vulnerabilities.[2] DOT and its Operating Administrations (OAs) agreed with our recommendations and have taken, or plan to take, corrective actions. While progress has been made, much remains to be done as shown in this report. The following summarizes key information security challenges that have a broad impact across DOT programs.

- ***Network Security***: The most significant network security issue we identified concerns FAA's plan to place its air traffic control systems, which now operate on a dedicated network, and its administrative systems on one integrated network with direct connections to the Internet. We found that while FAA asked vendors to propose security solutions for the integrated network, it did not adequately evaluate security for air traffic control systems. For example, among the 400 air traffic control systems, FAA only plans to have 40 systems certified as adequately secured prior to contract award, which was scheduled for October 2001.

---

[1] Top Twelve Management Issues, DOT, Report Number: CE-2000-026, December 20, 1999; Top Ten Management Challenges, DOT, Report Number: PT-2001-017, January 18, 2001.

[2] For security reasons, specifics concerning the weaknesses and our audit procedures are not discussed in this report, but were provided to DOT managers during all audits.

Another concern was that security evaluations performed on key air traffic control systems were based on the current dedicated network environment, not the proposed integrated network. We believe the solution is to combine all air traffic control networks, but leave FAA's administrative systems on separate networks. FAA has tasked an assessment team to perform a review of the proposed network security. Since we issued our report, FAA has announced that it is deferring the contract award until the security issue is resolved.

Another challenge facing DOT is the need to secure network entry points. We identified weaknesses in firewall security that allowed us to gain unauthorized access from the Internet to about 270 computers located within DOT's private networks. DOT took corrective action to strengthen firewall security. However, other entry points to DOT's private networks still are not secured. Contractors and industry associations are allowed access to DOT systems through direct network connections. DOT policy of obtaining security assurance from external parties is not being enforced.

- ***System Security***: More than 100,000 personnel (insiders), including DOT employees, contractor personnel, grantees, industry associations, and other Government agency personnel, are authorized to access DOT computer systems on its private networks. While DOT has strengthened network security to reduce the risk of unauthorized access from the internet, DOT systems are vulnerable to insiders. DOT lacks a critical control, which requires periodic management reviews to certify major systems are adequately secured to ensure integrity, confidentiality, and availability of system operations. Only about 10 percent of DOT mission-critical systems were reported to have received security certification reviews. We also found funding estimates for information security to be inconsistent and unsupported.

  The reported low percentage of reviews of system security is consistent with the result of our audits of selected systems. We identified internal control weaknesses within critical application systems. Examples included unlimited password attempts allowed, no automatic password expiration, password files not protected from "cracking," unauthorized remote access allowed, failure to use proper encryption standards to secure financial transactions, inadequate disaster recovery and system contingency plans, weak physical security, lack of oversight of contractors' work on the system, poor system documentation, lack of personnel background checks, and inadequate security plans. Most weaknesses should have been identified and corrected through security certification reviews by program officials.

- ***Critical Infrastructure Protection***: DOT identified 102 FAA systems and the facilities supporting the National Airspace System; 5 Coast Guard systems and

its Operations Systems Center; and the Saint Lawrence Seaway as critical infrastructure essential to the Nation's defense, economic security, or public confidence. As required by PDD-63, these critical assets need to be secured by May 2003. We identified at least one additional system at both FAA and the Coast Guard that should be designated as infrastructure critical assets.

We also found FAA did not adequately integrate physical and system security, and Coast Guard did not have adequate disaster recovery plans for PDD-63 systems. If its main data center experiences prolonged service disruptions, Coast Guard would have difficulty in recovering its search and rescue system, on which rescue authorities rely to obtain timely and accurate information on the positions and characteristics of vessels near a reported distress. Unless these issues are resolved timely, DOT may not be able to secure its infrastructure-critical assets by May 2003.

- ***Personnel Security***: Our review of personnel security for individuals authorized to access DOT computer systems on its private networks focused on background checks because of the large number of contractor personnel (about 18,000) working on DOT systems. FAA is responsible for the majority of these contractor personnel. Both GAO and OIG reported deficiencies in FAA contractor personnel background checks. We also reported that background checks are lacking in the rest of DOT. In July 2000, we made recommendations to both DOT and FAA for corrective actions. In August 2001, FAA reported that it has completed background checks on 85 percent of its contractor personnel, but the other OAs reported completion of background checks on only 25 percent of their contractor personnel.

- ***Web Security and Privacy Protection***: DOT has about 280 web servers supporting more than 150,000 web pages for public access. We identified significant vulnerabilities and privacy violations with DOT web sites. For example, we identified 109 high vulnerabilities that made DOT web servers susceptible to remote attack, 46 of which were associated with the "Top Ten Internet Security Threats" issued by the Federal Chief Information Officers Council. In response to our recommendations, DOT has made good progress in securing web sites and improving privacy protection of persons accessing its web sites. However, as evidenced by the recent Code Red Worm attack which caused service disruptions to more than 100 DOT computers including web sites, maintaining web security and privacy protection remains a challenge for DOT because of constant changes in technology and web development.

In our opinion, the combination of these deficiencies and vulnerabilities associated with DOT's information security program results in a material internal control weakness, which warrants reporting to OMB and Congress under the Federal

Managers' Financial Integrity Act of 1982. In addition to completing implementation of our prior audit recommendations, DOT needs to enhance security over network connections, enforce management reviews of major systems security, develop guidance for estimating and reviewing security funding for budget submissions, and re-assess its ability to meet PDD-63 requirements. The DOT Deputy Chief Information Officer agreed with our findings and has taken, or is taking, corrective actions on the six new recommendations made in this report.

SCOPE AND METHODOLOGY

Our audit focused on FAA air traffic control systems and Coast Guard search and rescue systems, DOT major financial systems, and DOT web security and privacy protection. We included results from 20 GAO and OIG audit reports and 5 testimonies on DOT computer security for about 3 years as of September 7, 2001.

We used the audit methodologies recommended by GAO and the President's Council on Integrity and Efficiency, and guidelines issued by other Government authorities such as the National Institute of Standards and Technology. We used commercial scanning software to assess DOT's network and web vulnerabilities and survey questionnaires to collect agencywide profiles on security related to computer systems, networks, and data centers. Information developed by DOT program officials and their contractors also was considered.

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Our work was performed between June and September 2001 at DOT Headquarters located in Washington, D.C.

ANALYSES AND RESULTS

Network Security

DOT employees, contractors, grantees, industry associations, and the public can access DOT computers through various network entry points. For example, the public can access DOT web sites through Internet entry points (front doors). Business associates also can access DOT computers through direct network connections (back doors). We found that DOT has made good progress in securing front doors to prevent unauthorized access by Internet users. However, DOT has weak controls over back doors. The most significant network security issue we identified concerns FAA's plan to place its air traffic control systems, which now operate on a dedicated network, and its administrative systems on one integrated network with direct connections to the Internet.

- We recently issued a report recommending that FAA not go forward with the network integration until it can give sufficient assurance that combining air traffic control systems with administrative systems on one integrated network will not compromise security of the National Airspace System.[3] To provide sufficient security assurance, both the network and all air traffic control systems connected to the network need to be evaluated together as one system because of interconnections among the systems.

  We found that while FAA asked vendors to propose security solutions for the integrated network, it did not adequately evaluate security for air traffic control systems. For example, among the 400 air traffic control systems, FAA only plans to have 40 systems certified as adequately secured prior to contract award, which was scheduled for October 2001.

  Another concern was that security evaluations performed on key air traffic control systems were based on the current dedicated network environment, not the proposed integrated network. We believe the solution is to combine all air traffic control networks, but leave FAA's administrative systems on separate networks. FAA has tasked an assessment team to perform a review of the proposed network security. Since we issued our report, FAA has announced that it is deferring the contract award until the security issue is resolved.

- DOT has 17 authorized Internet entry points and 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 web sites. We identified weaknesses in firewall security that allowed us to gain unauthorized access from the Internet to about 270 computers located within DOT's private networks.[4] DOT took corrective action to strengthen firewall security.

- DOT needs to strengthen security over direct network connections. Contractors and industry associations are allowed access to DOT systems through direct network connections. DOT's policy requires OAs to obtain written assurance from non-Federal entities certifying that their computer systems are in compliance with DOT security requirements for network connections.

---

[3] Report on Replacement of Telecommunications Systems, FAA, Report Number: FI-2001-076, August 21, 2001.

[4] Report on Headquarters Computer Network Security, DOT, Report Number: FI-2000-124, September 25, 2000.

We first reported the lack of compliance with this policy in August 1998.[5] In response to our recommendations, the DOT Office of the Chief Information Officer (OCIO) issued a memorandum requiring OAs to obtain written assurance from all external entities. However, we found compliance problems persist. For example, in August 2001, only two of seven OAs, which reported having third-party network connections, stated they were enforcing this policy requirement. Considering the ever-increasing complexity of network connections, the receipt of a statement from outside parties certifying their own network security may not provide DOT with meaningful assurance. DOT needs to enhance its guidance with specific evaluation criteria for OAs to use (Recommendation 1).

- GISRA specifically requires agencies to develop procedures for detecting, reporting, and responding to security incidents. These are critical controls to supplement firewall security. DOT has installed intrusion detection systems at major network entry points. We reviewed Coast Guard's intrusion detection and incident reporting operations and recommended that it develop better procedures for review coverage.[6] Our review of the access log for the Coast Guard key web site disclosed intensive hacking attempts from a foreign source. While the hacker was not able to break in, the intrusion detection personnel were not aware of the attempts.

  DOT should develop guidelines directing OAs to report security incidents to central Government authorities. For FY 2001, DOT recorded over 3,500 security incidents but reported only 2 to the General Services Administration's Federal Computer Incident Response Center (Recommendation 2).

System Security

More than 100,000 personnel (insiders) including DOT employees, contractor personnel, grantees, industry associations, and other Government agency personnel are authorized to access DOT computer systems on its private networks. While DOT has strengthened network access security to reduce the risk of unauthorized access from the Internet, DOT systems are vulnerable to insiders. A survey performed by the Federal Bureau of Investigations in 1998 reported that insiders constitute the greatest intruder threat. Our prior reviews also identified vulnerabilities to attack and abuse by insiders. For example, our Office of Investigations' work resulted in the prosecution of employees who embezzled

---

[5] Report on the Year 2000 Computer Program and Computer Security Challenges, DOT, Report Number: FE-1998-187, August 25, 1998.

[6] Report on Operations Systems Center Computer Security and Controls, U.S. Coast Guard, Report Number: FI-2001-089, September 7, 2001.

funds through stolen passwords, including one who embezzled $600,000 from DOT; and an employee who stole production software code used to operate an air traffic control system.

- DOT lacks a critical management control--security certification reviews--to ensure integrity, confidentiality, and availability of system operations. OMB requires agencies to perform periodic reviews to certify that major systems are adequately secured commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, information.

  This is a key control to ensure that information security is accomplished throughout the system life cycle. Both OMB and DOT policy require this review be performed before systems are placed into production (or upon major revisions) and every 3 years after implementation. While DOT has about 1,200 computer systems, it does not need, and may not be able to justify doing, periodic certification reviews for all of them. OMB and DOT policy require that managers select major systems to undergo periodic security reviews.

  We found no official record of DOT major systems for certification review, few security certification reviews performed, non-mission critical systems certified before mission-critical systems, and no formal plans to fix these weaknesses. We used the mission-critical systems listing developed for Year-2000 remediation as a baseline for our work. OAs reported that about 10 percent of systems and 6 percent of data centers have received security certification reviews. For major financial systems, only 24 percent have been certified as adequately secured for operations. These reported low percentages are consistent with our audits of selected systems.

  DOT also needs to better prioritize certification reviews. We found a wide range of management practices. For example, eight OAs did not perform any security reviews; one OA performed security reviews for all of its systems, both critical and non-critical; and two OAs had non-mission critical systems certified before mission-critical systems.

  In the FY 2002 Performance Plan, DOT established specific milestones for certifying the security for PDD-63 systems by May 2003. Recognizing the need to expand this commitment beyond PDD-63 systems, the departmental OCIO proposed to establish performance measures in the FY 2003 Performance Plan to have all DOT major systems certified by FY 2006. We support this initiative. However, until an official record of major systems is established and prioritized, DOT could not estimate the resources needed to meet this commitment (Recommendation 3).

- We also identified internal control weaknesses within critical application systems.[7] These weaknesses have a wide range of technical complexities and require different amounts of resources to fix. Examples included:

  - Management control weaknesses such as the lack of periodic security certification reviews and inadequate security policies.
  - Technical control weaknesses such as unlimited password attempts allowed, no automatic password expiration, password files not protected from "cracking," unauthorized remote access allowed, and failure to use proper encryption standards to secure financial transactions.
  - Operational control weaknesses such as weak physical security, the lack of disaster recovery and system contingency plans, no oversight of contractors' work, and poor system documentation.
  - Personnel control weaknesses such as the lack of background checks.

  While DOT has taken corrective actions to address the deficiencies identified, most weaknesses should have been identified and corrected through security certification reviews by program officials.

  One major corrective action undertaken by DOT was the removal of invalid user accounts from departmental financial systems. In 1999, we reported that hundreds of contractor employees retained access to DOT systems although they no longer worked on contracts for which their access was justified.[8] In response to our recommendation, FAA, who was responsible for controlling access to departmental financial systems, suspended about 300 user accounts, removed over 5,000 access privileges, and started certifying user access accounts every 6 months.

- DOT needs to develop guidance for estimating, tracking, and reporting system security funding. In 1996, Congress passed the Information Technology Management Reform Act (the Clinger-Cohen Act) which directed OMB to evaluate major capital investments made by agencies for information systems and to ensure agencies' information security policies, processes, and practices

---

[7] Report on Operations Systems Center Computer Security and Controls, U.S. Coast Guard, Report Number: FI-2001-089, September 7, 2001; Report on Finance Center Computer Security and Controls, U.S. Coast Guard, Report Number: FI-2001-088, September 6, 2001; Report on Implementing a New Financial Management System, DOT, Report Number: FI-2001-074, August 7, 2001; Report on Computer Security Controls of Financial Management System, Federal Transmit Administration, Report Number: FE-2000-098, May 23, 2000.

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

are adequate. OMB directed agencies to begin reporting computer security costs as a percentage of the total systems budget in the FY 2002 budget submission.

Proper development and reporting of budget estimates are critical to ensure information security is adequately funded. However, we found funding estimates provided by OAs to be inconsistent and unsupported. OAs reported a total of $44 million in the FY 2002 budget submission, but $51 million for GISRA reporting. The percentage of capital funding designated for security purposes also did not support the amounts reported in the budget submission. For example, FAA reported 3 percent of its capital funding ($2.1 billion) as designated for security purposes. Based on this percentage, FAA should have reported a total of $63 million, not $41 million, in its budget submission. Currently, there is no guideline to ensure the accuracy and supportability of security funding estimates (Recommendation 4).

Critical Infrastructure Protection

DOT identified 102 FAA systems and the facilities supporting the National Airspace System; 5 Coast Guard systems and its Operations Systems Center; and the Saint Lawrence Seaway as critical infrastructure essential to the Nation's defense, economic security, or public confidence. As required by PDD-63, these critical assets need to be secured by May 2003. We found that DOT may not be able to secure its infrastructure-critical assets by May 2003.

- DOT did not use any specific methodology, such as the Project Matrix methodology recommended by the Critical Infrastructure Assurance Office, to ensure comprehensive reviews of system dependencies when identifying critical assets. As a result, some systems were inappropriately excluded. For example, the Coast Guard's primary network system, on which other PDD-63 systems rely to operate, was not included. An FAA voice switching system, which is used to support controller-to-pilot communications, was not included because it is scheduled to be replaced in FY 2006. Only its replacement system is included as a critical asset for protection. FAA and Coast Guard agreed to develop plans to have these two systems secured by May 2003.

- While FAA has developed plans to certify system security by May 2003, it does not have a plan to ensure adequate physical security for the facilities housing PDD-63 systems. For example, many air traffic control systems operate at FAA en-route centers. FAA has completed the physical vulnerability assessments for these centers, but did not plan to complete elimination of identified vulnerabilities until FY 2006.

Another example is the long-range radar systems at more than 100 sites. FAA initially developed a timetable to certify only about half of these sites for physical security. While FAA recently agreed to accelerate the schedule for certifying physical security at en-route centers and long-range radar sites, a detailed plan supporting the accelerated schedule needs to be developed (Recommendation 5).

- Coast Guard has designated its main data processing center located in West Virginia as a critical asset, which supports PDD-63 search and rescue system and marine safety systems. However, Coast Guard does not have reliable disaster recovery and system contingency plans, or alternative processing facilities for use during emergency situations. If the data center experiences prolonged service disruptions, Coast Guard would have difficulty in recovering its search and rescue system, on which rescue authorities rely to obtain timely and accurate information on the positions and characteristics of vessels near a reported distress. Coast Guard agreed to take corrective actions.

Personnel Security

Common personnel controls on authorized users (insiders) include segregating key duties among staff, holding individuals accountable for actions, restricting individuals' access, and conducting background checks on individuals in positions of trust. Our review focused on background checks because of the large number of contractor personnel (about 18,000) working on DOT systems. While background checks provide no guarantee as to a person's loyalty or trustworthiness, they provide valuable information that might keep some personnel who are at risk from working on DOT systems. DOT has made good progress in catching up with necessary background checks; however, the work is not complete.

- In December 1999, 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. In September 2000, we testified before the House Science Committee that FAA needed to upgrade background checks on contractor personnel and develop firm milestones to complete the checks.[9]

  FAA originally concluded that about 90 percent of the contractor positions associated with its mission-critical systems were low risk and only required

[9] Statement of Inspector General Kenneth M. Mead before the Committee on Science, U.S. House of Representatives, Computer Security within DOT, Report Number: CC-2000-359, September 27, 2000.

fingerprint checks for disclosing possible criminal records. Based on our recommendation, FAA agreed to upgrade background checks to include financial checks due to the sensitivity of air traffic control systems. In August 2001, FAA reported that it has completed background checks on 85 percent of its contractor employees, including background upgrades for about 2,000 contractor personnel. As a result, FAA discharged about 250 contractor employees due primarily to financial problems disclosed by the more comprehensive background checks.

- Background checks also are lacking for contractor personnel employed by other OAs. We found that contractor personnel, who received no background checks, were tasked to perform sensitive work such as managing network security, grants payments, and search and rescue systems.[10] In August 2001, these OAs reported completion of background checks on only about 25 percent of contractor employees.

- Requirements for background checks were not consistently included in DOT contracts. DOT agreed to modify contracts by March 2001 to ensure the Government's rights to perform background checks. In August 2001, we reviewed a sample of 23 system-related contracts and found 3 (13 percent) contracts still had no background check requirements.

- We also found that DOT employees did not have the proper level of background checks required for their positions. DOT policy required different levels of background checks on Federal employees and contractor personnel based on designated position sensitivity levels. We reviewed 13 DOT Headquarters network systems that stored sensitive data and transmitted payment and payroll transactions. According to DOT policy, at least one position for each of the 13 network systems should have been designated as high risk and required extensive background checks. While 41 DOT employees were working on these networks, only 4 employees received more extensive background checks as required by the policy.

Web Security and Privacy Protection

The Federal Government is using the Internet more extensively for day-to-day operations, such as e-mail and information exchange. Congress also requires Government agencies to provide the option of electronic maintenance, submission,

---

[10] Report on Operations Systems Center Computer Security and Controls, U.S. Coast Guard, Report Number: FI-2001-089, September 7, 2001; Interim Report on Computer Security, DOT, Report Number: FI-2000-108, July 13, 2000; and Report on Computer Security Controls of Financial Management System, Federal Transit Administration, Report Number: FE-2000-098, May 23, 2000.

or disclosure of information as a substitute for paper by October 2003. We identified significant vulnerabilities and privacy violations with DOT web sites. In response to our recommendations, DOT has made good progress in securing web sites against attack and improving privacy protection of persons accessing its web sites. However, maintaining web security and privacy protection remains a challenge for DOT because of constant changes in technology and web development.

- DOT has about 280 web servers supporting more than 150,000 web pages for public access. Our reviews identified 109 high vulnerabilities that made DOT web servers susceptible to remote attack.[11] Forty-six of these vulnerabilities were associated with the "Top Ten Internet Security Threats" issued by the Federal Chief Information Officers Council. These vulnerabilities occurred because of weak configuration (setup) management controls. For example, 35 of the 46 high vulnerabilities could have been avoided if DOT had installed software fixes (patches) provided by software manufacturers.

  Attacks on DOT web sites could result in embarrassment (web sites defaced), inconveniences (web servers out-of service), or business disruptions (deleting reports filed by industry to meet regulatory requirements). In response to our recommendations, DOT took corrective actions and the departmental OCIO issued a "Server Security Checklist" to help OAs secure their web servers. However, securing web sites will be an ongoing challenge, as evidenced by the recent Code Red Worm attack which caused service disruptions to more than 100 DOT computers, including web sites.

- Web sites are excellent tools for the Federal Government to improve the quality of its services. However, until public users are confident that their privacy is protected, they will not use these services. In December 2000, Congress passed the FY 2001 Consolidated Appropriations Act which required the OIG at each Federal agency to report on the agency's collection and review of personally identifiable information on either the agency's Internet sites or through third-party agreements.

  Our review focused on "cookies," which is one of the principal technologies used to collect information from web visitors by placing small bits of software on web users' computers. GAO and our office identified unauthorized use of cookies on 23 DOT web pages due to improper software configuration or

---

[11] Report on Computer Security over Web Sites, DOT, Report Number: FI-2001- 061, May 23, 2001; Report on Headquarters Computer Network Security, DOT, Report Number: FI-2000-124, September 25, 2000.

improper default setting of the web development tool.[12] Although not intentional, this inadvertent use of unauthorized cookies was a privacy violation.

In response to our recommendations, the departmental OCIO issued a "Cookie Use Checklist" requiring annual certification by OAs to ensure web privacy protection. However, this remains a challenge to DOT because of constant web development activities. In August 2001, we reviewed a sample of 10 DOT web pages and found 1 unauthorized use of cookies.

In our opinion, the combination of these deficiencies and vulnerabilities associated with DOT's information security program results in a material internal control weakness, which warrants reporting to OMB and Congress under the Federal Managers' Financial Integrity Act of 1982 (Recommendation 6).

RECOMMENDATIONS

We recommend that the DOT Deputy Chief Information Officer:

1. Develop evaluation criteria for allowing network connections with external entities, and require OAs to assess all existing network connections based on the evaluation criteria.

2. Issue guidelines directing OAs to report security incidents to central Government authorities such as the General Services Administration's Federal Computer Incident Response Center.

3. Establish DOT's baseline of major systems requiring security certification reviews, assign priority to these systems, estimate resources needed, and develop performance measures for completing these certification reviews as part of the FY 2003 Performance Plan.

4. Issue guidelines for estimating security funding requirements for system projects, and establish procedures for evaluating system budget submissions for accuracy and supportability.

5. Work with FAA and Coast Guard to re-evaluate the identification of PDD-63 critical assets, and ensure a detailed plan is developed by FAA to accelerate

[12] Report on Web Privacy, DOT, Report Number: FI-2001-024, February 26, 2001; Report on Follow Up on Privacy Concerns for Web Visitors, Report Number: FI-2001-019, January 25, 2001; and Report on Privacy Concerns for Web Visitors, Report Number: FI-2001-006, November 2, 2000.

planned certification of physical security at en-route centers and long-range radar sites by May 2003.

6. Report DOT's information security program as a material weakness in the FY 2001 Federal Managers' Financial Integrity Act report to OMB and Congress.

PRIOR RECOMMENDATIONS

Since August 1998, we issued 13 other reports with recommendations to improve DOT's information security program. Key recommendations that we made to DOT and/or the OAs are summarized below and detailed in Exhibit C.

Network Security

- Do not go forward with network integration between air traffic control and administrative systems until FAA can provide sufficient assurance that combining the National Airspace System with administrative systems on one integrated network will not compromise security of the National Airspace System.

- Develop and implement intrusion detection review procedures to ensure comprehensive review coverage.

- Require OAs to disable Internet web services identified on 900 computers on DOT's private networks, and develop procedures to periodically examine DOT computers to prevent use of unneeded network services.

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

- Ensure outside users are in compliance with DOT security requirements.

System Security

- Enforce entity-wide security plan requirements and enhance employee training for conducting OMB Circular A-130 system certification reviews.

- Develop a schedule to have computer systems certified for adequate security, in accordance with DOT guidance.

- Improve password security by allowing limited password attempts, enforcing automatic password expirations, and protecting password files from "cracking."

- Improve remote network access security by eliminating uncontrolled use of remote network services.

- Improve access controls by automatically terminating inactive sessions.

- Upgrade security encryption planned for the new DOT accounting system.

- Identify and cancel all user accounts assigned to contractor and DOT employees who no longer work for DOT.

- Require all user accounts in the current security database be certified, and develop a policy for re-certification of employees and contractors.

- Review the authorized access list and limit unsupervised access to the computer room only to personnel who need to perform on-going technical work.

- Keep all computer room doors closed and locked.

- Develop and periodically test a comprehensive continuity of operations plan, including selection of a recovery site, as required by OMB Circular A-130.

- Store backup tapes in secure sites geographically distant from processing centers.

- Move the backup computer to a separate location from the primary computer.

- Turn on the operating system audit features and develop a management report listing all direct data changes made by contractor employees for management review and approval.

- Work with the contractor to ensure timely delivery of system design documentation and maintenance procedures as required in the contract.

- Document and follow formal procedures for reviewing, approving, and tracking software change requests.

Critical Infrastructure Protection

- Develop a schedule for evaluating, testing, and certifying PDD-63 systems and facility for adequate security by May 2003.

- Designate the Coast Guard Data Network (CGDN+) as infrastructure-critical and develop a plan to protect it by May 2003.

- Develop a more structured methodology, with a focus on system dependencies, for identifying potential PDD-63 systems. Re-evaluate Coast Guard systems, including newly deployed systems, and facilities for PDD-63 consideration.

Personnel Security

- Develop specific guidance for designating position sensitivity/risk levels for computer-related positions and incorporate the guidance into the DOT personnel security policy.

- Review existing contracts to ensure appropriate levels of background checks were done on contractor employees and, where not completed, implement a plan to do so.

- Include background check requirements in all future information technology contracts, and enforce these requirements.

- Identify key staff (either DOT employee or contractor personnel) responsible for maintaining, modifying, and securing Headquarters networks and complete higher level Background Investigation checks. Complete lower-level background checks on other staff involved in maintaining, modifying, and securing Headquarters networks.

- Upgrade the risk level of contractor positions associated with air traffic control systems.

Web Security and Privacy Protection

- 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.

- Use the Department's "Server Security Checklist" to enhance configuration management controls on existing computers, including timely installation of computer manufacturers' software fixes and upgrades.

- Require OAs to correct the vulnerabilities identified by OIG, and determine whether vulnerabilities exist and need to be corrected for other web servers.

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

- Issue the updated Cookie Use Checklist requiring periodical re-certification from OAs to ensure web privacy protection on DOT web sites.

- Require OAs to inform the DOT Chief Information Officer when experiencing inadvertent cookies introduced by web configuration or development tools. This information should be shared timely with all OAs.

DOT and the OAs agreed with all of our recommendations and are taking, or have taken, corrective actions.

MANAGEMENT RESPONSE

A draft of this report was provided to the DOT Deputy Chief Information Officer on September 4, 2001. He agreed with the new recommendations made in this report and will provide specific action plans and estimated completion dates in DOT's final GISRA submission to OMB.

OFFICE OF INSPECTOR GENERAL COMMENTS

Actions taken and planned by DOT are reasonable.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving DOT's GISRA corrective action plan upon its submission which currently is due to OMB by October 31, 2001. If you concur with our findings and recommendations, please state specific actions taken or planned for each recommendation and provide target dates for completion. If you do not concur, please provide your rationale. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

We appreciate the courtesies and cooperation of DOT and OA representatives. If you have questions concerning this report, please call me at (202) 366-1964 or John Meche at (202) 366-1496.

#

OIG INPUT TO THE GISRA EXECUTIVE SUMMARY

This section presents OIG input to meet the legislative mandate of the Government Information Security Reform Act (GISRA). OMB guidance requires that OIG (1) provide comments to DOT's Executive Summary for program reviews and independent evaluations, and (2) prepare a detailed independent evaluation report. Our independent evaluation report is provided separately. As required by OMB, we are commenting on 12 of the 14 items specified in the reporting guideline. The OIG review focused on actual performance of DOT's security program and practices.

STUDY 1 – SECURITY FUNDING

OIG was not required to respond to this item.

STUDY 2 – PROGRAMS INCLUDED IN INDEPENDENT EVALUATIONS

DOT has 14 OAs with a total of 1,200 computer systems. For the independent evaluations, OIG focused on:

- FAA air traffic control systems and USCG search and rescue systems, which support Federal programs deemed to have a high impact on the public by OMB. FAA and USCG also are responsible for all DOT critical infrastructure systems in accordance with PDD-63.

- DOT major financial systems, which are used to process billions of dollars of grant and contract payments. OIG found these systems were particularly vulnerable to insiders. Two employees recently were prosecuted for embezzling funds using stolen passwords, including one who embezzled $600,000.

- DOT web security and privacy protection, which involve more than 150,000 DOT web pages. Without adequate web security and privacy protection, the public would not fully use the services intended for E-Government and the Government Paperwork Elimination Act.

STUDY 3 – INDEPENDENT REVIEW METHODOLOGY

In making its independent evaluations, OIG included results from 20 General Accounting Office (GAO) and OIG audit reports and 5 testimonies on DOT

computer security for about 3 years as of September 7, 2001. OIG used the audit methodologies recommended by GAO and the President's Council on Integrity and Efficiency. OIG also used guidelines issued by other Government authorities such as the National Institute of Standards and Technology. For technical evaluations, OIG used commercial scanning software to assess DOT's network and web vulnerabilities. OIG also used a contractor to audit computer security at the USCG finance center.

Survey questionnaires were used to collect information from OAs to compile agencywide profiles on security related to computer systems, networks, and data centers. Information developed by DOT program officials and their contractors also was considered.

STUDY 4 – MATERIAL WEAKNESSES

Beginning in FY 2000, OIG identified computer security as one of the top management challenges facing DOT. OMB Circular A-130 requires agencies to adequately secure computer systems through the use of cost-effective management, personnel, operational and technical controls. OIG independent evaluations identified weaknesses in all four areas as summarized below.

- **Management Controls**: Enforcing computer security is a major challenge. While GISRA authorized creation of a senior management position for computer security in OCIO, this position has yet to be filled. For FY 2001, OCIO had only one full-time employee who, with assistance from contractors, was designated to enforce information security.

  OIG and GAO independent evaluations identified OA noncompliance with DOT security requirements. For example, as of August 2001, only about 10 percent of DOT's mission-critical systems have been reviewed for security certification although OMB and DOT have had long-standing requirements that all major systems be periodically reviewed for security certification.

  Other examples of noncompliance included allowing non-DOT entities to have network connections to DOT's private networks without proper security confirmation; placing contractor employees in key computer security positions without background checks; and placing public web sites on DOT's private networks.

- **Personnel Controls**: DOT's personnel security policy requires background checks on Federal employees and contractor personnel based on designated position sensitivity levels. While background checks provide no guarantee as to a person's loyalty or trustworthiness, they provide valuable information that might keep some personnel who are at risk from working on DOT systems.

  In December 1999, 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. In September 2000, OIG testified before the House Science Committee that other OAs also lacked background checks on contractor personnel. OIG found that contractor personnel, who received no background checks, were tasked to perform sensitive work such as managing DOT's network security. DOT, including FAA, initiated corrective actions to perform background checks on contractor personnel; however, the work is yet to be completed. OIG also found Federal employees did not have higher-level background checks required for their position.

- **Operational Controls**: Operational controls address implementation of security mechanisms to meet management control requirements. The most significant concern in this area is the pending decision on FAA's planned network replacement for air traffic control systems. Under FAA's proposal, air traffic control systems, which now operate on dedicated networks, would share the same network with administrative systems, which have direct connections to the Internet. Consequently, air traffic control systems would become more vulnerable to unauthorized intrusion.

  OIG recently issued a report recommending that FAA should not go forward with the network integration until it can give sufficient assurance that combining the National Airspace System with administrative systems on one integrated network will not compromise security of the National Airspace System. FAA has tasked an assessment team to perform an in-depth review of the proposed network security and is deferring contract award until the security issue is resolved.

  Another concern is that DOT may not be able to secure its infrastructure-critical assets by May 2003, as required by PDD-63. OIG independent reviews indicated that DOT had not adequately identified systems critical to the Nation's infrastructure, planned for the disaster recovery capability, or coordinated information security with physical security protection. For

example, the USCG data network and an air traffic control voice communication system should have been identified as infrastructure-critical. There was no alternative processing site or contingency plans for USCG search and rescue and marine safety systems. Also, FAA recently agreed to accelerate the schedule to fix physical vulnerabilities associated with PDD-63 critical assets. However, a detailed plan supporting the accelerated schedule needs to be developed.

- **Technical Controls**: OIG reviews identified weaknesses in firewall security, on which DOT relied to prevent unauthorized access by Internet users. In response to OIG findings, DOT has made good progress in securing Internet entry points (front doors); however, DOT still has weak controls over network connections with third parties (back doors) such as contractors and industry partners.

  OIG also identified 109 high vulnerabilities on DOT web servers, of which 46 were associated with the "Top Ten Internet Security Threats" issued by the Federal CIO Council; and use of unauthorized "cookies" on 23 DOT web pages. While the web vulnerabilities and unauthorized "cookies" identified by OIG have been fixed, maintaining web security and privacy protection remains a challenge to DOT because web sites are constantly revised.

  OIG's independent reviews also identified a lack of access controls in critical systems. Deficiencies found include insufficient password controls such as allowing unlimited password guesses, password files not protected, systems improperly configured allowing unauthorized remote access, and failure to use proper encryption standards to secure financial transactions. As a result, DOT systems are vulnerable to unauthorized access by insiders, including employees, contractor personnel, grantees, industry partners, and other Government employees.

STUDY 5 – PROGRAM OFFICIALS SECURITY PROGRAM

OMB asked about program officials' performance in assessing risk, determining appropriate level of security, maintaining up-to-date security plan, and testing and evaluating system security. All these tasks are required for performing system security certification reviews, as recommended by OMB Circular A-130. DOT policy requires program officials to conduct periodic system security certification reviews of major computer systems. However, there is no official record of DOT

major systems. OIG used the mission-critical system listing developed for Year-2000 remediation as a baseline for survey. OAs reported that about 10 percent of systems and 6 percent of data centers have received security certification reviews. For major financial systems, only 24 percent have been certified as adequately secured for operations.

Program officials also did not prioritize certification reviews. OIG found that one OA had conducted security certification reviews for all systems, almost half of which were non-mission critical; eight OAs did not conduct security reviews for any systems; and two OAs certified non-mission critical systems before mission-critical systems. The remaining three OAs have only certified about one-third of their mission-critical systems.

STUDY 6 – CIO SECURITY PROGRAM

Prior to the enactment of GISRA, OCIO issued guidance and polices for OAs to follow concerning various information security issues such as system certification reviews, continuity of operations planning, and personnel security. In response to GISRA requirements, OCIO established a formal information security program in May 2001.

In its Information Technology Security Program publication, OCIO provided comprehensive guidelines for information security implementation and required OAs to submit security action plans for review. In July 2001, OAs provided initial responses but they contained incomplete information. OCIO has not performed any assessment of the effectiveness of OA implementation plans. OCIO stated the new departmental senior computer security manager, when hired, will be responsible for effective implementation of the security program.

STUDY 7 – SECURITY TRAINING

Overall, DOT has provided comprehensive coverage for basic awareness training to almost all employees. For example, DOT stated in the FY 2000 Performance Report that about 95 percent of all DOT employees received security awareness training. For FY 2001, OAs reported about 99 percent of employees received awareness training. However, specialized training for people with security responsibilities needs to be accelerated.

The newly established information security program specified two important security positions—Information System Security Officers and System

Administrators. FAA and USCG are responsible for about 70 percent of DOT systems. So far, FAA has trained 25 percent of its Information System Security Officers and expects to have the remaining security staff trained by May 2003. USCG reported that it plans to complete training for all Information System Security Officers by the end of September 2001.

FAA reported it is in the process of identifying System Administrators. USCG reported about 300 System Administrators; however, it could not provide specifics on their training. The remaining OAs reported that about 90 System Administrators have received training, but were unable to provide the total number of System Administrators.

STUDY 8 – INCIDENT RESPONSE CAPABILITY

DOT does not have specific guidelines directing agencies to report security incidents to any central authorities. In an October 2000 memorandum, the Federal CIO Council and OMB recommended that agencies report externally generated security incidents to the General Services Administration's Federal Computer Incident Response Center (FedCIRC). For FY 2001, DOT recorded over 3,500 security incidents but reported only 2 to FedCIRC. Also, DOT should coordinate its security incident reporting to other Government entities. Currently, USCG reports to the Department of Defense for incidents related to its ".mil" web sites and FedCIRC for other incidents. FAA reports security incidents to the Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC).

DOT receives information regarding common vulnerabilities from multiple sources including FedCIRC, NIPC, and private companies. FAA shares this information with other OAs using weekly bulletins and alerts.

STUDY 9 – IT CAPITAL PLANNING

In the May 2001 Information Technology Security Program publication, OCIO required OAs to include information security as an integral part of investment decisions. For the FY 2002 budget submission, OMB directed agencies to start reporting the computer security cost as a percentage of the total systems budget. To meet this new reporting requirement, DOT needs to develop better estimating, tracking, and reporting procedures.

OAs provided inconsistent security funding estimates for FY 2002 between the Exhibit 53 budget submission ($44 million) and the GISRA report ($51 million). OIG found both estimates were unsupported. The $44 million included in the Exhibit 53 budget submission was based on the percentage of security funding reported by OAs for 420 capital planning projects. The percentage ranged from 0 to 25 percent. However, OAs could not provide details to support the percentages reported.

For the GISRA report, OAs reported both dollar amounts (totaling $51 million) and the aggregate percentage of OA capital funding designated for security purpose (ranging from 1 to 14 percent). However, the dollar amount and the percentage of funding reported do not support each other. For example, FAA reported that 3 percent of its capital funding ($2.1 billion) was designated for security purpose. Based on this percentage, FAA should have reported a total of $63 million, not $41 million, for FY 2002 security funding. The same problem exists with other OAs.

STUDY 10 – CRITICAL INFRASTRUCTURE PROTECTION

To meet PDD-63 requirements, DOT issued guidance defining critical assets. Based on this guidance, DOT identified 102 FAA systems and the facilities supporting the National Airspace System; 5 USCG systems and its Operations Systems Center; and the Saint Lawrence Seaway as PDD-63 critical assets requiring protection.

In identifying critical assets, DOT did not use any specific methodology, such as the Project Matrix methodology recommended by the Critical Infrastructure Assurance Office. OIG's independent review disclosed additional infrastructure-critical systems. For example, USCG's primary network system, on which USCG search and rescue and marine safety systems rely to operate, should have been identified as a critical asset for protection. Also, FAA needs to protect a critical air traffic control voice communication system, which will be operational until 2006. FAA identified only the replacement system as a critical asset.

STUDY 11 – SECURITY LIFE CYCLE

The key to ensure that information security is practiced throughout the system life cycle is by making periodic system security certification reviews. As stated in Study 5, with about 10 percent of mission-critical systems having received such

certification reviews, DOT needs to make a strong commitment to correct this deficiency. In the FY 2002 Performance Plan, DOT established specific milestones for reviewing and certifying the security for infrastructure-critical systems by May 2003. In preparing for the FY 2003 Performance Plan, DOT proposed to expand the plan to cover all systems requiring certification. OIG was told that the initial target is to have all these systems certified by FY 2006. However, until DOT develops an inventory of all major application systems and general support systems, such as data centers, requiring certification reviews, it could not estimate resources needed to meet the commitment.

STUDY 12 – SECURITY PROGRAM INTEGRATION

DOT needs to better integrate system security and physical security to protect critical air traffic control systems. In its critical infrastructure protection plan, DOT identified needs to protect both air traffic control systems and National Airspace System facilities by May 2003. While FAA has developed plans for reviewing, improving, and certifying information technology security in the air traffic control systems, it does not have a plan to ensure adequate physical security for the facilities housing these systems by the PDD-63 deadline.

For example, many air traffic control systems operate at FAA en-route centers. FAA has completed the physical vulnerability assessment for these centers, but did not plan to complete remediation and certification until 2006. Another example is the long-range radar systems supporting air traffic control operations at more than 100 sites. FAA initially developed a timetable to certify only about half of these sites for physical security. FAA recently agreed to accelerate the schedule for certifying physical security for en-route centers and long-range radar sites. However, a detailed plan supporting the accelerated schedule needs to be developed.

STUDY 13 – SUPPORTING SERVICES SECURITY

To ensure contractor-provided services are adequately secured, OIG reviews focused on background checks, network connection security, and removal of contractor employees' access to DOT systems. There are about 18,000 contractor employees working on DOT systems, of which about 17,000 work for FAA. During FY 2000, both GAO and OIG reported a lack of background checks on FAA contractor employees. Since then, FAA has made good progress and reported that it completed background checks on 85 percent of its contractor

employees. However, other OAs reported that only about 25 percent of contractor employees have received background checks. OIG also found that not all DOT procurement contracts have been modified to include contractual requirements for background checks, as recommended.

Contractor employees also were allowed access to DOT systems through direct network connections. DOT's policy requires agencies to obtain written assurance from non-Federal parties certifying that their computer systems are in compliance with DOT security requirements for network connections. OIG found that only two of seven OAs, which reported having third party network connections, stated they were enforcing this policy requirement.

In 1999, OIG reviewed user access accounts in DOT financial systems. OIG found that hundreds of contractor employees retained access to DOT systems although they no longer worked on the contract for which their access was justified. In response to the finding, FAA, who was responsible for controlling access to DOT systems, suspended about 300 user accounts, removed over 5,000 access privileges, and started certifying user access accounts every 6 months.

STUDY 14 – CORRECTIVE ACTIONS

OIG was not required to respond to this item.

OIG CONCLUSION

In view of the security weaknesses and concerns identified, OIG concludes that DOT information security represents a material weakness, and should be reported as such in DOT's FY 2001 Federal Managers Financial Integrity Act Report. Specifics about OIG findings, recommendations, and individual reports are detailed in the GISRA independent evaluation report submitted in conjunction with this Executive Summary.

REPORTS AND TESTIMONIES RELATED TO DOT COMPUTER SECURITY

Operations Systems Center Computer Security and Controls, OIG Report Number FI-2001-089, September 7, 2001.

Finance Center Computer Security and Controls, OIG Report Number FI-2001-088, September 6, 2001.

Replacement of FAA Telecommunications Systems, OIG Report Number FI-2001-076, August 21, 2001.

Implementing a New Financial Management System, OIG Report Number FI-2001-074, August 7, 2001.

DOT's 2000 Performance Report/2002 Performance Plan, OIG Report Number PT-2001-062, June 4, 2001.

Computer Security Over Web Sites, OIG Report Number FI-2001-061, May 23, 2001.

Statement of Kenneth M. Mead, Inspector General, Before the Subcommittee on Transportation and Related Agencies, Committee on Appropriations, U.S. House of Representatives, Management Oversight Issues, March 8, 2001.

Fiscal Year 2000 Consolidated Financial Statements, OIG Report Number FI-2001-037, March 1, 2001.

Web Privacy, OIG Report Number FI-2001-034, February 26, 2001.

Statement of Kenneth M. Mead, Inspector General, Before the Subcommittee on Transportation, Committee on Appropriations, U.S. Senate, Management Oversight Issues, February 14, 2001.

Followup on Privacy Concerns for Web Visitors, OIG Report Number FI-2001-019, January 25, 2001.

Top Ten Management Challenges, OIG Report Number PT-2001-017, January 18, 2001.

Major Management Challenges and Program Risks, GAO Report Number 01-253, January, 2001.

Privacy Concerns for Web Visitors, OIG Report Number FI-2001-006, November 3, 2000.

Statement of Kenneth M. Mead, Inspector General, Before the Committee on Science, U.S. House of Representatives, Computer Security within DOT CC-2000-359, September 27, 2000.

Statement of Joel C. Willemssen, Director, Civil Agencies Information Systems, Before the Committee on Science, U.S. House of Representatives, FAA Computer Security, GAO Report Number T-AIMD-00-330, September 27, 2000.

Headquarters Computer Network Security, OIG Report Number FI-2000-124, September 25, 2000.

Interim Report on Computer Security, OIG Report Number FI-2000-108, July 13, 2000.

Computer Security - FAA Is Addressing Personnel Weaknesses, But Further Action is Required, GAO Report Number AIMD-00-169, May 31, 2000.

Computer Security Controls of Financial Management System, OIG Report Number FE-2000-098, May 23, 2000.

Computer Security - FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software, GAO Report Number AIMD-00-55, December 23, 1999.

Top Twelve Management Issues, OIG Report Number CE-2000-026, December 20, 1999.

Computer Security Controls of Data Processing Center, OIG Report Number FE-1999-103, May 20, 1999.

The Year 2000 Computer Program and Computer Security Challenges, OIG Report Number FE-1998-187, August 25, 1998.

Statement of John L. Meche, Deputy Assistant Inspector General for Financial and Information Technology, Before the Subcommittee on Technology, Committee on Science, U.S. House of Representatives, FAA's Year 2000 Computer Program and Computer Security Challenges, FE-1998-187, August 6, 1998.

PRIOR AUDIT RECOMMENDATOINS

Audit Report Number: FI-2001-089, Operations Systems Center (OSC) Computer Security and Controls, September 7, 2001.

- Enforce Coast Guard entity-wide security plan requirements and enhance employee training for conducting OMB Circular A-130 system certification reviews.

- Develop a schedule by September 30, 2001, for evaluating, testing, and certifying PDD-63 systems and the OSC facility for adequate security by May 2003.

- Develop a schedule by December 31, 2001, to have other OSC computer systems certified for adequate security, in accordance with DOT guidance.

- Designate the CGDN+ network as infrastructure-critical and develop a plan to protect it by May 2003.

- Develop a more structured methodology, with a focus on system dependencies, for identifying potential PDD-63 systems. Re-evaluate Coast Guard systems, including newly deployed systems, and facilities for PDD-63 consideration based on this methodology.

- Identify and complete higher-level Background Investigations on key staff responsible for maintaining, modifying, and securing computer systems.

- Complete lower-level National Agency Check and Inquiry on all other Coast Guard and contractor employees.

- Require OSC to review the authorized access list and limit unsupervised access to the computer room only to personnel who need to perform on-going technical work.

- Improve password security by allowing limited password attempts, enforcing automatic password expirations, and protecting password files for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed.

- Improve remote network access security by eliminating uncontrolled use of remote network services for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether the same corrective actions are needed.

- Improve access controls by automatically terminating inactive sessions for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether the same corrective actions are needed.

- Correct all 150 confirmed vulnerabilities.

- Use the Department's "Server Security Checklist" to enhance configuration management controls on existing computers, including timely installation of computer manufacturers' software fixes and upgrades.

- Develop and implement intrusion detection review procedures to ensure comprehensive review coverage.

- For PDD-63 critical systems, OSC needs to use a reciprocal agreement with the Finance Center to be each other's recovery processing site, and work with system owners to develop system-level contingency plans in 6 months.

- Perform system recovery testing for PDD-63 systems in 12 months.

- Develop and test a disaster recovery plan, including selection of a recovery site, for all of its operations.

- Finalize the selection of a more geographically distant location to store backup files.

Audit Report Number: FI-2001-088, Coast Guard Finance Center (FINCEN), September 6, 2001.

- Develop and implement a plan and schedule to certify financial systems and the data center in accordance with OMB Circular A-130.

- Develop and periodically test a comprehensive continuity of operations plan as required by OMB Circular A-130. This plan should include alternative

processing arrangements or facilities and an offsite storage facil
tapes at a sufficient distance from the data center.

- Improve security over password files, and establish procedures for periodic review of users' need to access financial systems.

- Document and follow formal procedures for reviewing, approving, and tracking software change requests.

Audit Report Number: FI-2001-076, Replacement of FAA Telecommunications Systems (FTI), August 21, 2001.

- Do not go forward with network integration between air traffic control and administrative systems until FAA can provide sufficient assurance that combining the National Airspace System with administrative systems on one integrated network will not compromise security of the National Airspace System.

- Require that the assessment team consider cost-benefits and FAA's capability of supporting network security over the life of FTI in making recommendations for FAA consideration.

- Integrate only the networks supporting air traffic control operations, but consolidate the support and management functions for all of the air traffic control and administrative networks.

Audit Report Number: FI-2001-074 Implementing a New Financial Management System, August 7, 2001.

- Implement and test Delphi's disaster recovery and business continuity plan and upgrade Delphi's security encryption.

Audit Report Number: FI-2001-061 Computer Security Over Web Sites, May 23, 2001.

- Establish June 8, 2001, as the deadline for OAs to correct all confirmed high, medium, and low potential vulnerabilities.

- Expedite the issuance of the web configuration management cor
  so that OAs can certify the security of their web servers befor
  servers for use.

Audit Report Number: FI-2001-034 Report on Web Privacy, February 26, 2001.

- Issue the updated Cookie Use Checklist requiring periodical re-certification from DOT agencies to ensure web privacy protection on DOT web sites.

- Require DOT agencies to inform the DOT Chief Information Officer when experiencing inadvertent cookies introduced by web configuration or development tools. This information should be shared timely with all DOT agencies.

Audit Report Number: FI-2001-019, Follow Up on Privacy Concerns for Web Visitors, January 25, 2001.

- Incorporate provisions in DOT's web configuration checklist for building connections to non-Government web sites and revising existing web sites. Web sites experiencing major revisions should be subject to the same review and approval process as new web development projects.

- Require the OAs to review their existing web design by January 31, 2001, to ensure that automatic linkage to non-Government web sites is not being used.

- Work with FAA to ensure persistent cookies detected on FAA web pages are immediately disabled and steady progress is made to ensure FAA's compliance with DOT web privacy policy by January 31, 2001.

Audit Report Number: FI-2001-006, Report on Privacy Concerns For Web Visitors, November 3, 2000.

- Require OAs to disable use of persistent cookies identified on their web sites, including the ones they intend to justify for continued use, until the Secretary's approval has been obtained.

- Require OAs to check all web pages for potential use of cookies, and report the total number of web pages checked before certifying compliance.

- Accelerate the development and release of the web configura concerning the use and approval of cookies.

Audit Report Number: FI-2000-124, Headquarters Computer Network Security, September 25, 2000.

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

- Notify DOT internal agencies to disable Internet web services on the 900 computers we identified.

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

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

- 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.

- 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.

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

Audit Report Number: FI-2000-108, Interim Report on Computer Security, July 13, 2000.

- Develop specific guidance for designating position sensitivity/risk levels for computer-related positions and incorporate the guidance into the DOT personnel security policy.

- Review existing contracts to ensure appropriate levels of background checks were done on contractor employees and, where not completed, implement a

plan to do so, and issue a notice to all DOT Contracting Officers include such requirements in all future information technology enforce these requirements.

- Identify key staff (either DOT employee or contractor personnel) responsible for maintaining, modifying, and securing Headquarters networks and complete higher level Background Investigation checks on these individuals, and complete lower-level NACI background checks on other staff involved in maintaining, modifying, and securing Headquarters networks.

- Upgrade the risk level of contractor positions associated with air traffic control systems by September 30, 2000.

- Develop a workable plan, in cooperation with Federal investigation agencies, with firm milestones to complete background checks on contractor personnel.

Audit Report Number: FE-2000-098, Report on Computer Security Controls of Financial Management System, Federal Transit Administration, May 23, 2000.

- Program the computer system to require passwords changes at regular intervals and to automatically suspend user access accounts after three unsuccessful password attempts.

- Keep all computer room doors closed and locked.

- Identify key employees responsible for the integrity and continuity of operations and obtain background investigations.

- Incorporate the personnel security background check requirement in the contract, and obtain proper background checks on contractor employees.

- Instruct the contractor to turn on the operating system audit features and develop a management report listing all direct data changes made by contractor employees for review and approval.

- Work with the contractor to ensure timely delivery of system design documentation and maintenance procedures as required in the contract.

- Move the backup computer to a separate location from the primary computer.

- Take daily backup tapes to a secure location.

- Initiate appropriate action to certify and accredit this mission-cri
  December 2000.

Audit Report Number: FE-1999-103, Computer Security Controls of Data Processing Center, May 20, 1999.

- Remind FAA employees who authorize contractors' access to the data center of their responsibility to terminate such authorizations when access is no longer needed.

- Identify and cancel all user accounts assigned to contractor and DOT employees who no longer work for DOT.

- Require all user accounts in the current security database be certified, and develop a policy for re-certification of employees and contractors.

- Restrict access to the report generator to security representatives as defined in FAA's Mainframe Security Handbook.

- Determine whether the four vulnerable network programs should be disabled or modified.

Audit Report Number: FE-1998-187, The Year 2000 Computer Program and Computer Security Challenges, August 25, 1998.

- Provide for physical separation of the primary and backup replacement computers.

- Ensure outside users of DOT computer networks are in compliance with DOT security requirements.

- Develop schedules to certify computer systems and install network security evaluation tools.