Office of Inspector General

Interim Report on Computer Security

Department of Transportation

Report Number: FI-2000-108
Date Issued: July 13, 2000

Memorandum

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

Subject: ACTION: Interim Report on Computer Security, DOT FI-2000-108

Date: July 13, 2000

Reply To Attn Of: Meche:x61496

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

To: Assistant Secretary for Administration, DOT
Chief Information Officer, DOT
Federal Aviation Administrator

The Inspector General was invited to testify on June 14, 2000, before the Committee on Science, United States House of Representatives, on computer security within the Department of Transportation (DOT). The Committee postponed the hearing until September 2000—the month the Federal Aviation Administration (FAA) plans to achieve a significant milestone for improving its personnel security. We decided to issue the substance of the testimony prepared for the hearing as an interim report with recommendations for corrective actions.

As more fully discussed below, these recommendations pertain to performing background checks on contractor personnel, upgrading background checks on DOT and contractor employees, and ensuring that contracts have appropriate language requiring background checks and that contracting officers enforce the contract requirements for background checks.

RESULTS-IN-BRIEF

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

Needing Background Checks on Authorized Users

We found DOT needs to strengthen background checks on personnel (Government and contractor) authorized to access DOT's private systems. A survey performed by the Federal Bureau of Investigation in 1998 reported that insiders constitute the greatest intruder threat. Our recent reviews of a financial system and 13 network systems identified a general lack of background checks on contractor personnel and a lack of appropriate background checks on employees throughout DOT.

DOT's personnel security policy includes four different levels of background checks based on designated position sensitivity level or risk level. According to DOT policy, key personnel authorized to access these systems should receive more extensive Background Investigations (BI), while others should receive lower-level National Agency Check and Inquiry (NACI) background checks[1]. We found:

- Financial Management System: A total of 34 DOT employees and contractor personnel are responsible for maintaining, modifying, and securing this system. The more extensive BI background check was not conducted on any DOT employees, and no background checks were done on any contractor personnel.

- Network Systems: A total of 102 DOT employees and contractor personnel are responsible for maintaining, modifying, and securing 13 Headquarters network systems. We found only 4 employees were designated as occupying high-risk positions and received corresponding BI background checks. For contractor personnel, we found a wide range in levels of background checks including 1 BI check, 5 fingerprint checks, and no background checks on the remaining 55 contractor personnel.

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. FAA has agreed to bring its contracts into compliance with the personnel security policy by:

- Completing risk assessments and initiation of background checks on all people working on all mission-critical systems by September 30, 2000. However, a full plan for completing all background checks is not now in place. FAA needs to develop a workable plan with firm milestones to complete background checks on contractor personnel.

[1] Background Investigation (BI) checks require personal interviews and cost $2,300 to $2,700.
National Agency Check and Inquiry (NACI) checks require only documentation reviews and cost $77.

- Considering upgrading the level of background checks on contractor personnel. FAA originally assessed that about 90 percent of contractor positions associated with 72 mission-critical systems were low risk. The minimum background check requirement for low risk positions is a fingerprint check against the Federal Bureau of Investigation's crime database.

In our opinion, FAA should upgrade the level of contractor background checks because of the sensitivity of air traffic control systems.

Closing Security Weaknesses in DOT Networks

We also identified network security weaknesses that made DOT's systems vulnerable to unauthorized access by Internet users. Specifically:

- By logging on as non-DOT Internet users, our staff gained unauthorized access to over 250 DOT computers located within DOT's private network area. DOT is taking action to close this vulnerability.

- While most of DOT web sites intended for public viewing were placed in separate areas, 13 of them were inappropriately placed on DOT's private networks. When we brought this to management's attention, these public web sites were removed from DOT's private networks.

Accessing FAA's National Airspace System (NAS)

The current networks supporting FAA's NAS operations are relatively immune from intruders because of the networks' physical isolation. However, as part of the NAS modernization, FAA is considering replacement of these physically isolated networks with an integrated network supporting both administrative and NAS operations. This planned action requires FAA to install sophisticated network access controls and to examine whether air traffic control systems connected to the integrated network require security upgrades. Until it can give assurances that NAS security will not be compromised, FAA should not go forward to integrate the NAS and administrative systems on a common network.

This report contains recommendations to enhance personnel security. Key recommendations are:

- Develop and implement specific guidance for designating position sensitivity/risk levels for computer-related positions throughout DOT,

- Include requirements for background investigations in DOT contracts and ensure appropriate levels of background checks are done,

- Identify key DOT and contractor employees who need the higher level BI checks and complete their background investigations, and

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

We will issue separate reports with recommendations for improving DOT and FAA network security.

BACKGROUND

The Office of Inspector General (OIG), recognizing the importance of computer security, reviewed DOT's network security in 1997. We found DOT lacked firewalls to prevent Internet users from navigating DOT's networks, or using these networks to gain access to other computers. Since then, DOT installed firewalls to secure the 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 a December 1999 report[2] 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.

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 the planned IT expenditures. DOT has over 600 mission-critical systems, including safety-sensitive air traffic control systems, Coast Guard search and rescue systems,

[2] Top 12 Management Issues--Department of Transportation, dated December 22, 1999 (Report Number CE-2000-026).

and financial systems supporting the accounting for, and distribution of, billions of dollars in Federal funds. DOT's annual budget is about $50 billion. 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 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.

ANALYSES AND RESULTS

Thousands of people are authorized to access DOT computer systems on its private networks, including DOT employees and grantees, contractors, 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. To ensure integrity, confidentiality, and availability of computer operations, adequate personnel controls have to be established in conjunction with management controls (e.g., control policies and procedures); operational controls (e.g., physical security, contingency planning); and technical controls (e.g., access security, network intrusion/detection).

Common techniques for personnel controls 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.

DOT Needs to Strengthen Background Checks on Authorized Personnel

DOT's personnel security policy[3] includes four different levels of background checks on employees, based on designated position sensitivity level or risk level.

[3] DOT Order 1630.2A, entitled "Department of Transportation Personnel Security Handbook." FAA Order 1600.1D, entitled "Personnel Security Program" contains similar requirements as DOT Order 1630.2A.

The policy provides specific guidance on computer-related positions. Most 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 employees) Fingerprint check (for contractors)	NACI check (see above) Fingerprint check includes: ➢ Checks against FBI criminal records ➢ $18 to $28 in costs

Background Checks on DOT Authorized Users

OIG recently completed a review of a DOT financial system and is currently reviewing 13 Headquarters 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 employees 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 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 code 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 employees[4].

- 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 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 employees 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, 34 received at least the NACI background checks. Three employees did not receive any background checks. DOT is taking action to obtain background checks on the three employees.

  Of the 61 contractor personnel, we found a wide range in levels of background checks. One Coast Guard contractor received the extensive BI background check. Five FAA contractors received fingerprint checks to obtain building entrance passes. Other contractors 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 background checks were not

[4] OIG Report entitled "Computer Security Controls of Financial Management System--Federal Transit Administration," dated May 23, 2000 (Report Number: FE-2000-098). Management agreed to take appropriate actions to meet DOT's personnel security requirements.

consistently included in DOT contracts. DOT management has agreed to correct these problems.

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 employees, and must have contracting officers enforce compliance.

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, and is considering upgrading the level of background checks on contractor employees.

Having proper background checks on contractor personnel is important to FAA in view of the multi-billions of dollars of work done by contractors. FAA contractors work on systems critical to the safety and stability of the NAS, such as writing, repairing, and testing of computer code. For example, contractors work on software-intensive systems such as the Wide Area Augmentation System (WAAS)—a satellite system using the Global Positioning System technology, and the Standard Terminal Automation Replacement System (STARS)—a commercially 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. As reported by FAA, it must take four steps to obtain assurance of contractor personnels' backgrounds. FAA plans to complete its work on contract identification, risk assessment, and contract modifications and initiate background checks for contractor personnel working on its 435 mission-critical systems by September 2000.

FAA reported 297 mission-critical systems do not require any additional security assessment because the contracts are closed, or there were no personnel associated

with the contracts. The remaining 138 systems are in various stages of review, as shown in Table 2.

Table 2

Work Needed	Target Completion	No. of Systems
1. Identify Associated Contracts	7/21/00	10
2. Complete Risk Assessment for Contractor Position	8/15/00	56
3. Modify Contracts and Initiate Background Checks	9/30/00	72
4. Conduct Background Checks	Open	Open

FAA is in the process of initiating background checks for contractor personnel on 72 systems. FAA originally concluded about 90 percent of these contractor positions are low risk. However, FAA is considering an upgrade of contractor positions' sensitivity level and type of background checks.

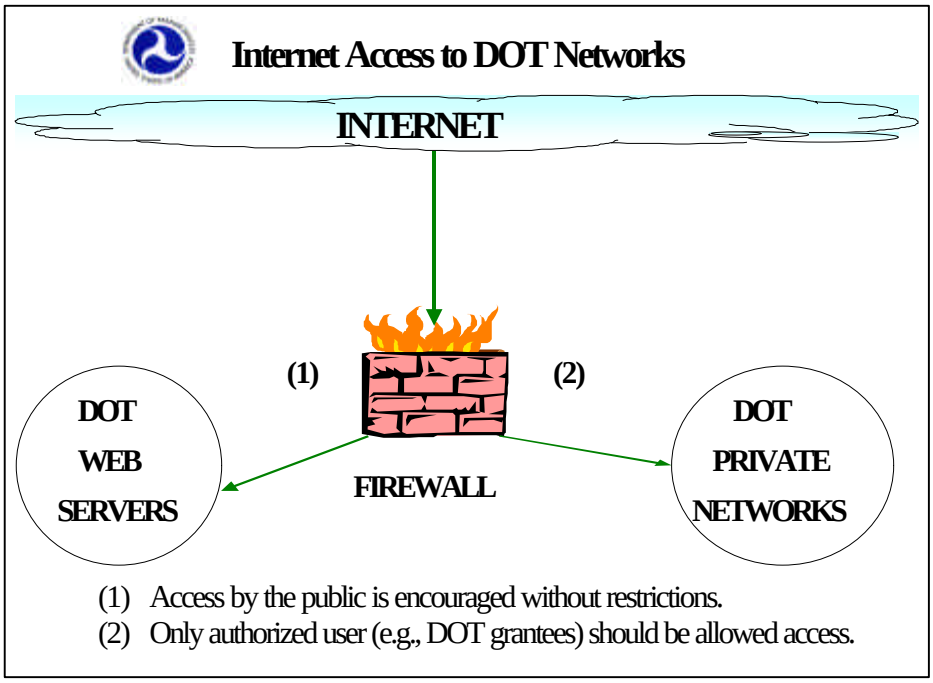
The minimum background check requirement for low risk positions is a fingerprint check against the Federal Bureau of Investigation's crime database. Higher risk levels would require additional background checks such as recent employment, education, and financial condition. In our opinion, FAA should upgrade the level of contractor background checks because of the sensitivity of air traffic control systems. Since the type of background check is a critical element in estimating how much time is needed to complete checks on all contractors, FAA should finalize this decision by September 30, 2000.

While FAA has made progress in recent months, much remains to be done. Because this is a sizable task, FAA needs to develop a workable plan with firm milestones to complete background checks on contractor personnel. A full plan is not now in place. FAA needs to prioritize the work based on system criticality and position sensitivity. It will be some time before background checks are completed on contractor personnel. Once background checks are complete, more time may be needed to take management actions such as removal of personnel from contracts, if warranted.

DOT Needs to Strengthen Network Security to Prevent Unauthorized Access

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

Table 3



Because DOT's computer networks are highly interconnected, it is extremely important that only authorized users are granted access. OIG identified security weaknesses in both current and planned future network environment.

Access to DOT Networks

Our ongoing audits[5] have identified the following weaknesses, which made DOT's private networks vulnerable to unauthorized access by Internet users:

- By logging on as non-DOT Internet users, OIG gained access to over 250 DOT computers located within DOT's private network area. None of these computers reside in FAA or Coast Guard Headquarters. DOT is taking action to close this vulnerability.

[5] The ongoing audits focus on Headquarters network operations. Computer security over FAA and Coast Guard field operations will be covered in future audits.

- 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. None of these belong to FAA or Coast Guard. When we brought this to management's attention, these web sites were removed from DOT's private networks.

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 that could result in deleting or changing data in computers, 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 and increase employees' security awareness training to prevent recurrences of these problems. We will be making recommendations to enhance DOT computer security in our upcoming reports.

Access to FAA's National Airspace System

As reported by the President's Commission on Critical Infrastructure Protection[6], the current networks supporting the NAS operations are relatively immune from intruders because of 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. During our ongoing FAA Telecommunications Infrastructure (FTI) review, we found that FAA is currently considering replacement of its isolated network with an integrated network.

[6] 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.

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 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 29 systems, but system assessments for all the remaining systems will not be completed until September 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.

RECOMMENDATIONS

We have ongoing reviews of DOT's network computer security and FAA's network replacement project (FTI) and plan to issue separate reports with specific recommendations for improving network security. Therefore, we are only making recommendations for improving personnel background checks in this report.

We recommend that the DOT Assistant Secretary for Administration:

1. Direct the Office of Security and Administrative Management, in cooperation with the Chief Information Officer, to develop specific guidance for designating position sensitivity/risk levels for computer-related positions and incorporate the guidance into the DOT personnel security policy for consistent application throughout DOT.

2. Review existing contracts, in cooperation with Operating Administrations, to:

    a) Ensure appropriate levels of background checks were done on contractor employees and, where not completed, implement a plan to do so.

    b) Issue a notice to all DOT Contracting Officers of the need to include such requirements in all future information technology contracts, and enforce these requirements when included in contracts.

We recommend that the DOT Chief Information Officer:

3. Work with Operating Administrations' Information Resources Management Offices to:

    a) 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.

    b) Complete lower-level NACI background checks on other staff (DOT employee and contractor personnel) involved in maintaining, modifying, and securing Headquarters networks.

We recommend that the FAA Administrator:

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

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

ACTION REQUIRED

In accordance with Department of Transportation Order 8000.1C, we would appreciate receiving your written comments within 30 working days. If you concur with our findings and recommendations, please indicate for each recommendation the specific action taken or planned, and the 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 representatives. If you have questions or require additional information concerning this report, please call me or Rebecca Leng at (202) 366-1496.

-#-