Office of Inspector General

Audit Report

Computer Security Controls of Financial Management System

Federal Transit Administration

Report Number. FE-2000-098
Date Issued: May 23, 2000

Memorandum

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

Subject: ACTION: Report on Computer Security Controls of Financial Management System, FTA FE-2000-098

Date: May 23, 2000

Reply To Attn Of: Meche:x61496

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

To Acting Federal Transit Administrator

This report presents our audit results on a Federal Transit Administration (FTA) financial management computer system[1]. Our audit objective was to determine whether computer security controls are adequate to ensure the operational integrity and service continuity of the FTA computer system. This audit was performed in conjunction with our Chief Financial Officers Act responsibilities to opine on the Fiscal Year (FY) 1999 Highway Trust Fund Financial Statements.

RESULTS IN BRIEF

The FTA system's computer security controls were not adequate to ensure operational integrity and continued operations. Using a widely known user identification "code," we were able to gain unauthorized access to the system's primary computer. As a result, FTA changed the access code.

We also identified seven system weaknesses and vulnerabilities: (1) passwords that should have expiration dates did not, and FTA allowed unlimited guesses at passwords; (2) computer rooms were not secure; (3) appropriate background checks for FTA and contractor employees were not performed; (4) FTA was not using the computer system's built-in audit trail software features to monitor the contractor's work; (5) FTA was overly dependent on contractor employees to make programming modifications; (6) the primary and backup computers were in the same room and backup tapes were not properly secured offsite; and (7) the computer system was not certified and accredited as a secure system.

[1] For security reasons, specifics concerning the computer system and our audit procedures are not discussed in this report, but were discussed in detail with FTA management.

These vulnerabilities occurred because FTA had not assigned a sufficient priority to computer security. These security weaknesses could significantly reduce FTA's ability to carry out its business mission and could cause FTA to lose its automated capabilities to maintain financial, project oversight, and operational control. FTA agreed with our findings and recommendations, and has taken or is taking corrective actions.

BACKGROUND

The FTA computer system uses a mini-computer operated at an offsite location by a contractor. FTA designated the computer system as mission-critical. It also is a sensitive system because the loss, misuse, or unauthorized access to, or modification of, the computer system would be harmful to the agency's mission. As such, certain levels of physical and computer security must be obtained to protect the computer system and the data it processes. DOT requires its sensitive systems to undergo system certification and accreditation ("authority to operate") procedures.

SCOPE AND METHODOLOGY

We evaluated procedures over computer security effectiveness of physical, password, and personnel controls. We interviewed FTA and contractor representatives. We performed on-site inspections of contractor and FTA computer facilities and equipment to verify proper security configuration. We tested computer access controls and evaluated FTA's capability for continuity of service. This audit was performed between January and March 2000 in conjunction with our audit of the FY 1999 Highway Trust Fund Financial Statements.

We conducted the audit using the General Accounting Office's (GAO) Federal Information Systems Computer Audit Manual. The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Audit work was performed at FTA Headquarters in Washington, D.C. and the contractor site.

ANALYSES AND RESULTS

Computer Security

The recent experience with Year-2000 computer problems reminded the world how much our business and personal lives depend on interconnected computer systems. Congress also has proposed legislation to strengthen information security

practices throughout the Federal Government[2]. We tested computer security to determine whether physical, password, and personnel controls were adequate to protect the system. We found improvements are needed.

- Network security. The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," requires Federal computer systems be secured from unauthorized access. FTA management stated an extended shutdown of the computer system would have major consequences to its business mission. Using a widely known user identification "code," we gained unauthorized access to the FTA system from a DOT computer. We did not gain access from outside DOT. We brought this issue to FTA's attention, and they quickly fixed it.

- Password Security. Federal Information Processing Standards Publication 112, "Password Usage," recognizes weaknesses associated with passwords and sets a standard for password use. Because password security can be easily compromised (stolen or guessed), the same password should be used for only a short time. To keep unauthorized users from guessing at passwords, computer systems should be programmed to automatically suspend access after three unsuccessful password attempts.

  There are about 3,300 authorized system users who can create or delete information. Users have to authenticate their identity by entering proper passwords when accessing the system. However, the system passwords do not expire and unauthorized users can make unlimited attempts to guess the password, thereby increasing the risk of unauthorized access.

- Physical Security. DOT Order 1350.257, "Departmental Guide to Physical/Environmental Security Planning," states one issue to be considered as a physical access control is to restrict normal access with barriers and screening measures at each entry point. Computer equipment used to support the system operations is located at FTA Headquarters and the contractor site. FTA has two computer rooms, one that houses communications equipment used to support field operations and the other contains equipment used to transfer money.

  Physical security at FTA Headquarters was inadequate. While the computer room doors had cipher locks installed, we observed the doors were left open at various times of the day. With this open access, computer equipment is at risk to theft, misuse, or intentional damage. Physical access controls at the contractor site were adequate.

[2] Government Information Security Act of 1999 (S.1993)

- Personnel Security. DOT Order 1630.2A, "Department of Transportation Personnel Security Handbook," and corresponding policy memoranda define position sensitivity and background security check requirements for DOT employees and contract personnel working in computer-related positions. The FTA computer system is mission-critical, involving the accounting, disbursement, or authorization of billions of dollars per year. According to DOT policy, key computer staff should have a Background Investigation[3] that requires an update every 5 years. For those whose technical work is reviewed by higher authority, they should have a lower level background check[4] that requires no updates.

  We found 18 DOT employees and 16 contractor personnel, including 3 foreign nationals, are responsible for maintaining, modifying, and securing the system operations. However, only the lower level background check was performed on DOT employees with two exceptions[5] and no background check was performed on any contractor personnel. The system contract also did not contain any provision for background checks on contractor personnel. Without adequate background checks, management has no assurance that reliable people are placed to manage this mission-critical system.

- Oversight of Contractor's Work. DOT Order 1350.271, "Guide to Information Protection for Senior Managers," recommends audit trails be established for DOT systems to ensure only authorized changes are made. A special update software could be used to directly modify computer data, such as authorized amount, without going through the normal update process that is recorded in an audit trail report. While this update software was designed for legitimate reasons such as emergency fixes, its use has to be carefully controlled.

  We found three contractor personnel could use this software. However, the system tracking audit features were turned off. As a result, FTA management had no mechanism to know when this special update software was used, who used it, what was changed, or whether only authorized changes were made.

[3] A Background Investigation (BI) is required for staff occupying a position with "significant involvement in mission critical systems." A BI check involves personal interviews, costs $2,300, and takes 6 to 12 months to complete.

[4] A lower level background check—National Agency Check and Inquiry (NACI)—is required for staff occupying a position which is "under technical review of higher authority." A NACI check is limited to a documentation review, costs $77, and takes 4 to 6 months to complete.

[5] One employee received a Background Investigation in 1971, which has not been updated. The other employee received no background check.

System Continuity of Service

Recent high profile hacker attacks on major companies' computer systems highlighted how vulnerable computers are in today's interconnected network environment. We found that without improved system documentation and contingency planning, the FTA system's service continuity was at risk.

- System Maintainability. National Institute of Standards and Technology Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," states proper documentation such as functional requirements, program specifications, and procedural documents should be maintained for computer systems. This FTA computer system is a database management system with over 700 program modules. However, FTA employees do not have the design documentation, nor are they familiar with the technical procedures used to make system changes.

  FTA depends on the contractor to maintain and enhance the computer system. If the current contract support becomes unavailable, FTA would experience difficulties in fixing operational problems or upgrading the system to meet new requirements. FTA has requested the contractor provide complete system documentation by September 30, 2000.

- Backup and Off-site Storage Procedures. OMB Circular A-130 requires continuity of operations planning for every information system in order to rapidly and effectively deal with potential disruptions of mission-critical and business functions. The system's primary and backup computers are located at the contractor site in the same room and only a few feet apart. The lack of physical separation poses the risk of losing both computers in case of a fire or natural disaster.

  The system's contingency plan requires that FTA have a backup computer in FTA Headquarters. While FTA has a designated computer room with proper communications lines installed in its Headquarters, we found arrangements for installing a backup system had not been made.

  DOT Order H1350.273, "Guide to Information Protection for Contractors," requires backup computer files be generated regularly and stored in a secure location. In case of disasters or operational problems, computer operations could be recovered from these backup files. The contractor creates daily backup tapes. However, a contractor employee takes the backup tapes home for storage. FTA could lose these backup tapes if the employee's home is damaged by fire or burglarized.

System Certification and Accreditation

OMB Circular A-130 requires that management use a systematic approach to evaluate the adequacy of computer system security. DOT Order H1350.253, "Departmental Guide to Certification/Accreditation of Information Systems," provides detailed guidance on assessing whether controls and security in a computer system are commensurate with the risk resulting from the loss, misuse, unauthorized access to, or modification of, the FTA system. The FTA computer system has been operational since November 1998; however, it has yet to be certified and accredited for adequate controls and security.

Five control items are specified in the DOT guidance for system certification and accreditation evaluation. The table shows weaknesses identified in this report were directly related to these evaluation items.

Table 1--Certification and Accreditation Evaluation Items

Findings	Management Controls	Operational Controls	Technical Controls	Development Controls	Security Training*
Network Security			X		
Password Security			X		
Physical Security		X			
Personnel Security	X	X			
Oversight of Contractor's Work			X		
System Maintainability		X			
Backup and Off-site Storage		X			
Certification and Accreditation				X	

* Currently being conducted by FTA.

Accordingly, FTA could have discovered these weaknesses had it instituted the process to certify and accredit this mission-critical system.

RECOMMENDATIONS

We recommend that the Acting Federal Transit Administrator:

1. Direct the contractor to program the FTA computer system to require passwords changes at regular intervals and to automatically suspend user access accounts after three unsuccessful password attempts.

2. Direct the system project manager to keep all computer room doors closed and locked.

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

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

5. 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 FTA review and approval. The report should list when the change is made, the person who made the change, and the content of the change.

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

7. Require the system project manager to move the backup computer to a separate location from the primary computer.

8. Direct the contractor to take daily backup tapes to a secure location agreeable to FTA and the contractor.

9. Initiate appropriate action to certify and accredit this mission-critical system by December 2000.

MANAGEMENT RESPONSE

A draft of this report was provided to the Acting FTA Administrator on April 28, 2000. FTA agreed and provided these comments:

Recommendation 1: FTA has implemented controls to automatically suspend user access accounts after three unsuccessful password attempts. FTA also was developing the password expiration date feature during the period of the OIG review. The computer system contains the "change your password after 90 days" expiration date feature, and is currently being tested. The expiration date feature is scheduled to be released in late May 2000, and fully deployed by August 2000.

Recommendation 2: During the period of the OIG review, the computer room experienced a failure with the building's cooling equipment. FTA has had the cooling equipment replaced and the door secured with a cipher lock. Access to this room is controlled to a limited number of staff, and an entry log is maintained to record all entries.

Recommendation 3: FTA will take appropriate action to meet this requirement.

Recommendation 4: FTA will work to ensure the contractor selected and the Statement of Work (SOW) for fiscal year 2001 includes the background check requirement. The current contract staff undergo an internal background check prior to hiring. This includes requiring a written questionnaire to be returned by all prior employers, verification of all prior schooling, three reference checks, and financial background checks.

Recommendation 5: During the period of the OIG review, audit trail software was being tested by FTA, and FTA's Security Officer was developing an implementation plan. As of April 25, 2000, the "Windows Security Event Auditing" feature has been activated. The implementation of the feature employs extensive use of transaction history tables, journals that record changes to data records, a checkpoint process for committed changes to data records, and there are "footprints" on the information records that document the date, time, and individual who changed the information.

Recommendation 6: On September 27, 1985, all FTA staff who were classified as computer specialists in their position description had their positions abolished through the departmental A-76 action. Since that action, all positions for computer operations, system maintenance, and applications support have been out-sourced by FTA. To maintain an operational knowledge of application programs and management processes, FTA has been scheduling training sessions with the maintenance contractor, and has rotated work assignments of government staff to include offsite hands-on training with contractor support staff. In addition, FTA has secured contract services with two other contractors who are qualified to maintain the FTA system.

The contractor has submitted the midyear revised work plan including system documentation and operational procedures. This plan is currently under review by the Office of Information Technology.

Recommendation 7: There is a certified server, located in FTA's Headquarters, that has supported the production system in the past. FTA intends to use this server as the backup machine in case computers at the contractor site become unavailable.

Recommendation 8: FTA backup tapes for the closing periods are stored at the departmental disaster recovery vendor site. FTA has made arrangements to store the nightly backup tapes in a secure area within the contractor's facility.

Recommendation 9: Obtaining the security accreditation is a flagship initiative within FTA. FTA began developing the requirements for the SOW and negotiating the cost of the three major deliverables required by OMB Circular A-130 in November 1999. The SOW is in the third review by FTA's Information Systems Security Officer.

OFFICE OF INSPECTOR GENERAL COMMENTS

Actions taken and planned by FTA are reasonable. Corrective actions already have been completed for Recommendations 2, 5, 7, and 8. We request that FTA provide estimated completion dates within 30 days for planned and ongoing actions for Recommendations 3, 4, 6, and 9.

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

-#-