COMPUTER SECURITY OF DELPHI FINANCIAL MANAGEMENT SYSTEM

Department of Transportation

Report Number: FI-2003-094
Date Issued: September 30, 2003

Memorandum

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

Subject: ACTION: Report on Computer Security of Delphi Financial Management System, Department of Transportation FI-2003-094

Date: September 30, 2003

From: Alexis M. Stefani
Principal Assistant Inspector General for Auditing and Evaluation

Reply to Attn. of: JA-20

To: Acting Assistant Secretary for Budget and Programs/Chief Financial Officer

This report presents the results of our audit of computer security over the Department of Transportation's (DOT) new financial management system—Delphi. In 1997, DOT decided that its existing accounting system did not meet DOT's need to properly account for resources and provide timely and reliable financial information to managers. DOT then embarked on an effort to acquire a commercial off-the-shelf financial management system that fully complied with Federal financial management and accounting requirements.

The replacement system, known as Delphi, provides significantly improved financial management and reporting capabilities. For example, billions of dollars worth of accounting adjustments that had to be manually processed outside the old accounting system are now being processed by Delphi. DOT will be able to produce financial statements from Delphi directly. Financial management staff can also access Delphi for information with web design technologies. When fully implemented, Delphi will be used to account for over $50 billion of funds entrusted to DOT each year, including over $10 billion in contractor and employee payments.

All DOT Operating Administrations (OA) have implemented Delphi, except the Federal Aviation Administration (FAA), which is scheduled to convert to the new system in October 2003. Delphi is maintained by FAA personnel at the Mike Monroney Aeronautical Center (Aeronautical Center) in Oklahoma City, under the

direction of the Office of the Secretary's Office of Financial Management. The system cost about $100 million to develop and deploy.

The objective of this audit was to determine whether Delphi is adequately secured to ensure the integrity, confidentiality, and availability of its operations. Specifically, we assessed the following control areas: (1) security planning to ensure that Delphi security risks are properly assessed; (2) access security to ensure Delphi files, documents, and facilities are accessible only to authorized personnel with proper separation of duties; (3) system software settings to ensure firewall, network, database, and transmission controls are adequate; (4) configuration management controls to ensure that only authorized changes can be made to Delphi; and (5) business continuity and contingency plans to ensure the plans are adequate and have been tested.

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Our audit scope and methodology are discussed in Exhibit A.

DOT provided comments (see Appendix) to our August 29, 2003 draft report. DOT concurred with all 5 findings and 17 recommendations in our report and has initiated or completed corrective action for each recommendation.

RESULTS IN BRIEF

Delphi has significantly improved DOT's ability to account for funds and to generate financial information. However, DOT needs to enhance security and controls of Delphi operations in order to achieve the full potential of the replacement system. Specifically, we found that some DOT employees could process unauthorized payments without being detected, and intruders could launch attacks as "trusted parties[1]" through unsecured network connections.

We also determined that critical security measures, such as protecting sensitive information from unauthorized disclosure, were not implemented or enforced. In addition, changes made to Delphi were not properly tested and reviewed, which could result in unauthorized program changes or system performance degradation. Finally, contingency planning was not adequate to ensure continued Delphi services in the event of a disaster.[2]

---

[1] "Trusted parties" are users who are granted access to DOT's network or system resources that are not made available to the general public.

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

These deficiencies existed because DOT did not pay adequate attention to security issues during the Delphi development process. Instead, the focus has been on assisting OA conversion efforts and enabling OAs to use Delphi for financial statement reporting. Our review showed that while the vulnerabilities uncovered are significant, they are also correctable. To that end, DOT has initiated or completed corrective actions on many of the deficiencies we identified. Continued management attention will be required to complete the remaining corrective actions and to provide ongoing assurance that security controls remain adequate to protect sensitive information and resources from being compromised or lost.

Based on the existence and magnitude of these vulnerabilities, we conclude that the control environment for Delphi operations must be improved. Accordingly, when auditing DOT financial statements, auditors will need to perform additional testing of financial transactions processed by Delphi.

- **User Access Needs to Be Restricted to Ensure Payment and Financial Reporting Integrity.** Controls over payment processing in Delphi were inadequate due to a lack of separation of duties. In financial systems, no single individual should be given the authority to both request and approve payment. However, we found 35 Delphi users were given authority to perform both payment request and approval functions without any management review.

  The number of users authorized to both request and approve payments could increase to about 100 when FAA converts to Delphi. Currently, 61 FAA employees have this authority to perform both functions, but the risk of unauthorized payments was mitigated by a customized system control in the old accounting system, which prohibited individuals from approving their own payment requests. In contrast, Delphi is largely a commercial off-the-shelf system and does not have the same customized control. Accordingly, separating payment request and approval functions must be enforced in Delphi to prevent one individual from both submitting and approving a transaction. Implementing this separation of duties would require realignment of job responsibilities in FAA accounting offices before the conversion.

  We also found that an excessive number of DOT and contractor employees at the Aeronautical Center were given system privileges that were not required to perform their duties. As a result of these privileges, about 200 support personnel could change accounting records without management approval or install malicious software code in Delphi that could result in service disruptions.

  In addition, over 400 Aeronautical Center employees had unsupervised physical access to the Delphi computer center, although about half were not

responsible for Delphi operations. Once inside the computer center, these employees could cause disruptions by issuing special commands on operator consoles or sabotaging computer equipment.

During our audit, we did not identify any specific incidents of unauthorized payments, accounting transactions, or software installations in Delphi. DOT management has started enforcing separation of payment request and approval functions at each OA and reducing system access assigned to support personnel. Continued management attention is required to complete corrective actions.

- **Network Security Needs to Be Strengthened to Prevent Outside Intrusions.** We found over 30 vulnerabilities on the 2 web sites through which Delphi receives transactions for processing. These vulnerabilities allowed intruders to access sensitive information that could be used to gain unauthorized access to, or launch attacks on, Delphi.

  We also found that the local area network at the Aeronautical Center was vulnerable to attack. Although the network was protected by firewall security[3] against intrusions from the Internet, it was accessible through other remote access mechanisms. We found over 120 unsecured telephone line (dial-up modem) connections to the network. With such connections, intruders could launch attacks as "trusted parties" to disrupt Aeronautical Center network operations. While these unsecured connections were not found on Delphi computers, they were threats to Delphi because Delphi has to rely on the Aeronautical Center network for communications support.

  DOT management has eliminated all vulnerabilities we identified on Delphi web sites and disconnected 35 unsecured dial-up connections. Action plans need to be developed and implemented to secure the remaining connections and to prevent recurrence of these problems.

- **Security Controls Need to Be Enforced to Ensure Processing Integrity.** We found that basic system controls were not implemented in Delphi. When compared with the old accounting system, Delphi lacked basic security controls such as implementing proper password configuration to prevent guessing, automatically deleting user accounts not used over a designated period of time, or systematically removing terminated employees from system access. These deficiencies existed partially due to a change in the system processing environment. Delphi operates on a stand-alone server, which

[3] While firewall security helps prevent unauthorized access to an organization's private networks, it cannot protect public web sites from being attacked.

requires that security controls that are normally provided by a central security function (as was provided for the old accounting system) must now be performed by Delphi managers.

In addition, the following requirements in the Delphi security plan have not been enforced.

- Protecting sensitive information. While most sensitive Delphi data are encrypted during transmission, we found incidents where employees' Social Security Numbers and purchase card information are transmitted over DOT networks in clear text and, if intercepted, can easily be copied. In addition, tens of thousands of employees' Social Security Numbers stored in Delphi for the expense reimbursement process are not protected. Over 400 Delphi users can access this sensitive information, which reduces employee privacy and risks identity theft. Unless this information is properly protected, the magnitude of this exposure will increase significantly when FAA converts to Delphi.

- Ensuring integrity of system interfaces. We found little evidence to show that DOT has ensured that feeder systems, providing Delphi with detailed financial data, are secure. A critical security requirement for Delphi is that these feeder systems provide evidence of adequate security before being allowed to share information with Delphi. We found that three of eight feeder systems we selected for testing did not have any evidence of adequate security. While the other five had such evidence, only one provided it to Delphi management.

- Enforcing personnel accountability. We found that DOT did not hold individuals accountable for keeping Delphi secure. The Delphi Security Plan requires that DOT and contractor employees accept security responsibilities by signing "rules of behavior" documents before being given access to Delphi. Such rules include not sharing passwords with others and not disclosing sensitive information. We selected two OAs for review and found that one was not aware of, and the other did not consistently comply with, this requirement. As a result, management will not be able to hold employees and contractors accountable for security breaches.

- Conducting background checks. While background checks do not guarantee a person's loyalty or trustworthiness, they provide valuable information to help management determine whether an employee should be given access to Delphi. We reviewed 14 individuals occupying sensitive positions, such as maintaining network security, and found that 8 (about

57 percent) DOT and contractor employees have not received adequate background checks.

These security deficiencies existed because the Delphi security administrator did not enforce security requirements specified by management. The administrator is four levels below the Director of Delphi operations at the Aeronautical Center and was focused on detailed administrative work such as processing user access requests.

DOT is taking corrective actions such as enforcing proper password configuration and ensuring that all interfaces are adequately secured. To help improve security administration, DOT has now appointed a Delphi information system security officer who will report to a higher level of authority. DOT management needs to continue implementing security controls necessary in Delphi, such as using secure mechanisms to transmit sensitive information, protecting employee Social Security Numbers stored in Delphi, obtaining DOT and contractor employees' signatures on the rules of behavior, and completing proper background checks on personnel occupying sensitive positions.

- **System Changes Need to Be Better Controlled.** While the Delphi team used a structured process to control system changes, we found that this process needed to be strengthened because testing was inappropriately performed on the production machine,[4] key personnel were not involved in prioritizing change requests or assigning staff to review test results, and critical testing documents were not retained for future reference.

  System changes should be made, tested, and reviewed in a test environment, and only approved changes should be accepted and placed on the Delphi production machine. While Delphi development staff performed detailed testing on a test machine, they conducted the final testing, such as quality assurance testing, on the production machine. This arrangement resulted in two immediate concerns. First, problems experienced during testing could have an adverse impact, such as performance degradation or system crashes, on the Delphi production machine. Second, to ensure that only approved changes are implemented on the production machine, system development staff responsible for making program changes should not be allowed to access the production machine. This separation of duties did not exist for Delphi.

  Delphi had a Change Control Board (the Board) responsible for approving and prioritizing change requests and assigning personnel to review test results.

[4] The Delphi production machine is the computer that is used to process financial transactions submitted by DOT Operating Administrations.

However, the Board was composed of only system development personnel at the Aeronautical Center without any OA user representation. As a result, DOT had limited assurance that Delphi incorporated only necessary changes requested by the users. Also, the Delphi security administrator was not involved to ensure that security was not negatively affected during a change. In one instance, password security was inadvertently degraded during a system change, but it was not detected for over 1 year until it was pointed out during our audit.

While there was evidence that the Board reviewed and signed off on system changes, we found that test plans and results were not retained. Without such documentation, the Delphi team might experience additional difficulties when researching future system problems.

As a result of our audit, DOT management has removed the test database from the Delphi production machine. However, further DOT management attention is needed to have OAs represented on the Change Control Board for reviewing Delphi change requests and test results, require the security administrator to ensure that security is not degraded during system changes, and develop a policy for retaining system change documents based on the criticality of the change.

- **Contingency Plans Need to Be Enhanced and Tested.** The April 2001 Delphi contingency plan was not adequate to ensure continued payment and accounting operations in DOT in case of a major catastrophe at the Aeronautical Center. The plan called for using an on-site portable computer center as backup, which would not work if a disaster placed the entire Aeronautical Center out of service. We also identified the need for the Aeronautical Center to reduce its risk of losing major telecommunications lines. While these communication lines used different entry points into the Aeronautical Center, they converged in a single room before entering the data center. Losing this room would leave Delphi inaccessible to all OA users.

  During our audit, DOT management revised the Delphi contingency plan by selecting an off-site facility for recovery processing. DOT performed limited off-site tests on July 27 and September 7, 2003. However, management needs to develop a plan to eliminate converging major telecommunications lines in a single room at the Aeronautical Center.

We are making specific recommendations in this report to enhance computer security over the Delphi system. These include recommendations to ensure payment and reporting integrity in Delphi, reduce vulnerabilities to attack from

outside intruders, add basic security controls to Delphi, ensure integrity of program changes in Delphi, and test contingency plans.

Management fully concurred with our findings and recommendations and, to its credit, is taking corrective actions that, when fully implemented, will significantly enhance the integrity, confidentiality, and availability of DOT financial operations. These corrective actions are in various stages of implementation. In some instances, DOT management has completed corrective actions such as revising Delphi's contingency plan for improved disaster recovery capability and appointing a Delphi information system security officer who reports to a higher level authority. All other recommendations are scheduled to be implemented by December 2003.

FINDINGS AND RECOMMENDATIONS

A. User Access Needs to Be Restricted to Ensure Payment and Financial Reporting Integrity

DOT did not establish appropriate system access controls to protect financial information stored in Delphi. Specifically, we found a lack of separation of duties between requesting and approving payments in Delphi, and excessive system and physical access granted to Aeronautical Center support personnel. As a result, DOT employees and contractors could embezzle funds by processing unauthorized payments, change accounting records without management approval, or install malicious software code in Delphi. During our audit, we did not identify any specific incidents of unauthorized payments, accounting transactions, or software installations in Delphi.

Lack of Separation of Duties in the Payment Process

Controls over payment processing in Delphi were inadequate due to a lack of separation of duties. In financial systems, no single individual should be given the authority to both request and approve payments. However, we found 35 Delphi users in 4 OAs and at the Aeronautical Center were given authority to perform both payment request and approval functions without any management review.

The number of users authorized to both request and approve payments could increase to about 100 when FAA converts to Delphi. Currently, 61 FAA employees have authority to perform both functions. However, under the old accounting system, the risk of unauthorized payments was mitigated by a customized system control, which prohibited individuals from approving their own payment requests. In contrast, Delphi is largely a commercial off-the-shelf system and does not have the same customized control. Accordingly, separating payment request and approval functions must be enforced in Delphi to prevent one individual from both submitting and approving a transaction. Implementing this separation of duties would require realignment of job responsibilities in FAA accounting offices before the conversion.

Excessive System Access to Delphi by Support Personnel

We found that an excessive number of DOT and contractor employees at the Aeronautical Center were given access to Delphi's financial records or operating system although such access was not required for their duties. As a result of this access, 182 DOT and contractor employees responsible for Delphi operations at the Aeronautical Center could change accounting records without OA approval or

install malicious software code in Delphi that could result in service disruptions. Specifically, system support personnel could:

- Change accounting records. We found that 71 system support personnel could bypass detailed transaction processing controls and make direct changes to OA general ledger account balances. While some Delphi system support personnel may need to have such access for emergency adjustments, the access should be limited and monitored. For example, an exception report listing all changes should be provided to the OA for review.

  Also, 61 of these individuals could make changes to prior-year accounting records without management review and approval after the records have been closed. Once financial statements have been certified by auditors, they should be closed permanently. Any changes that need to be made should be processed as prior-year adjustments. As a result of these excessive access privileges, OAs had limited assurance of the integrity and accuracy of their financial records.

- Change operating system software. We found that the majority (111 out of 122) of Delphi technical support personnel were inappropriately granted access to the operating system that is used to control Delphi operations. This excessive access presented a risk because these individuals could install malicious software code that could result in disruptions to the Delphi system.

  Equally important, we found that 5 of the remaining 11 individuals that had legitimate needs to access the Delphi operating system were arbitrarily deleting the audit trails of their access activities. This prevented management from holding these users accountable for changes made to the Delphi operating system.

Excessive Physical Access to the Delphi Computer Center

Only personnel responsible for performing technical work, such as monitoring computer operations or maintaining hardware, should be given unsupervised access to the computer center. However, we found that over 400 Aeronautical Center employees were granted unsupervised physical access to the Delphi computer center, even though most of these individuals were not responsible for ongoing operations or maintenance of the computer equipment in the center. Many of these individuals, such as 91 security guards and 40 building maintenance staff, only needed to enter the computer room occasionally, and therefore should be given temporary access, when needed.

Once inside the computer center, these employees could cause disruptions by issuing special commands on operator consoles or by simply sabotaging computer equipment. When compared with other computer centers, physical access security at the Aeronautical Center was inadequate. For example, U.S. Coast Guard's main computer center houses more systems than the Aeronautical Center, but unsupervised access was granted to less than one-third of those allowed for the Delphi computer center.

As a result of our audit, DOT management has started enforcing separation of payment request and approval functions at each OA and reducing privileged access assigned to support personnel. Continued management attention is required to complete corrective actions.

RECOMMENDATIONS

We recommend that the Acting Assistant Secretary for Budget and Programs/Chief Financial Officer direct the Office of Financial Management to:

1. Separate the payment request and approval authority for the 35 employees who currently have authority to do both, ensure that FAA follows the same separation of duties guidelines before it converts to Delphi, and install a process to ensure the separation of request and approval authority.

2. Determine which of the 71 system support personnel at the Aeronautical Center require privileged access to Delphi accounting records, eliminate privileged access for the remainder, and implement an exception report listing transactions made by personnel who retain this access for OA management review.

3. Eliminate all unnecessary access to Delphi's operating system for the remaining support personnel we identified at the Aeronautical Center.

4. Establish procedures that require audit trails of user access to the operating system be kept for a certain period of time and periodically reviewed by management.

5. Reduce the number of staff granted unsupervised physical access to the computer center to a small group of personnel responsible for operating and maintaining the computer equipment in the center.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

DOT has completed action on recommendations 1 and 5, and expects to complete action on recommendations 2, 3, and 4 by December 2003. The actions taken and in process are responsive to the recommendations.

B. Network Security Needs to Be Strengthened to Prevent Outside Intrusions

We found that Delphi web servers were not securely configured to prevent unauthorized access by non-DOT personnel. In addition, people outside DOT could access the Aeronautical Center network, which supports Delphi communication operations, without going through firewall security checks. As a result, intruders could make unauthorized changes to the Delphi system or disrupt its communication services.

Delphi Web Sites Unsecured

Delphi receives transactions through two web sites—one is accessible through the Internet and the other is accessible through DOT's internal networks. Through these Delphi web sites, users can make inquiries, request payments, or update fund accounting records in the Delphi database. If not properly configured, these web sites could allow unauthorized access to Delphi.

By using a commercial scanning tool, we identified over 30 vulnerabilities on the Delphi web sites. These vulnerabilities could allow intruders to bypass Delphi security checks and make unauthorized changes to the Delphi database by executing remote commands. These weaknesses occurred because Delphi's web sites were not properly configured as recommended by the National Institute of Standards and Technology and the software manufacturer, such as replacing vendor-supplied passwords with individual passwords.

DOT management has eliminated all vulnerabilities we identified and is working with the software manufacturer to ensure proper configuration of Delphi web sites.

Aeronautical Center Network Vulnerable to Remote Access

The Aeronautical Center provides the network infrastructure supporting Delphi communication operations. If the network is disrupted, Delphi will be out of service. Although the Aeronautical Center network was protected by firewall security against intrusions from the Internet, it was not protected from other remote access mechanisms.

By using a commercial software tool, we found 124 unauthorized telephone line connections (known as dial-up modems), which could allow individuals located outside of DOT to make connections with Aeronautical Center computers without going through firewall security. Once connected, intruders could launch attacks as "trusted parties" to disrupt Aeronautical Center network operations. For example,

by using these dial-up connections, we were able to connect to and execute commands on these computers from outside of DOT.

Only 11 of the 124 dial-up modems required password authentication, and none of them used the call-back mechanism to validate the calling source, as required by DOT policy. At the time we identified the 124 dial-up modems, DOT management was not aware of their existence and did not have a procedure in place to authorize the use of modems. While these unsecured dial-up connections were not directly associated with Delphi, they presented a threat to Delphi operations because Delphi relies on the Aeronautical Center network for communications support.

The Aeronautical Center management has completed its review of all dial-up modems we identified and disconnected 35 of them. Currently, DOT is determining appropriate actions for the remaining modems.

RECOMMENDATIONS

We recommend that the Acting Assistant Secretary for Budget and Programs/Chief Financial Officer direct the Office of Financial Management to:

1. Verify that Delphi web sites are securely configured, and periodically inspect the Delphi web configuration to prevent recurrence of vulnerabilities on Delphi web sites.

2. Complete corrective actions on the remaining dial-up connections.

3. Establish a process to control the use of dial-up modems in accordance with DOT policy.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

DOT has completed action on recommendation 1 and expects to complete action on recommendations 2 and 3 by December 2003. The actions taken and in process are responsive to the recommendations.

C. Security Controls Need to Be Enforced to Ensure Processing Integrity

We found that basic system security controls were not implemented in Delphi. For example, users were allowed to select short, simple passwords that could be easily guessed; unused user accounts were not removed; and access was not automatically removed when an employee was terminated. In addition, requirements specified in the Delphi security plan to protect sensitive information; ensure system interface integrity; and require personnel accountability and background checks were not enforced. As a result, DOT did not have adequate assurance about the integrity and confidentiality of information processed in Delphi.

Lack of Basic System Controls

Delphi lacked basic system controls that had been in place in the old accounting system partially due to a change in the system processing environment. While the old accounting system operates in a shared mainframe environment equipped with a central security management function, Delphi operates in a dedicated server environment. This transition imposed additional responsibilities on Delphi management for security implementation. We found the following basic system controls were missing in Delphi.

- Password configuration control. Password controls are generally considered a system's first line of defense against unauthorized access. According to DOT policy, passwords are required to contain at least eight alpha-numeric characters to prevent easy guessing. However, this control did not exist in Delphi. For example, during our Delphi testing, we were able to construct passwords with only three characters, which could easily be cracked by a hacker.

- Automatic time-out. Systems such as Delphi should automatically disconnect a user after a specified period of inactivity, such as 15 minutes. Without this control, unauthorized users can access unattended computers to process fraudulent transactions. This is evidenced by an embezzlement in recent years where an employee was able to use his supervisor's computer, while unattended, to approve fraudulent payment requests in the old accounting system.

- Disabling unused accounts. While user accounts not used for 90 days are suspended in Delphi, they can be re-activated no matter how long the accounts have stayed inactive. Once an account reaches 180 days of inactivity, the account is not likely to be needed and should be removed to prevent unauthorized use.

- Removing terminated employees' access. The old accounting system has the ability to match terminated employee records reported by the personnel system with a list of authorized users and remove their access. However, the Delphi system has no systematic way to remove the access of terminated Federal employees. As a result, we found that four employees still retained access to Delphi after termination from DOT.

DOT is taking corrective action to establish proper password configuration. However, DOT needs to continue implementing the remaining basic system controls such as disconnecting inactive sessions, deleting inactive user accounts, and systematically removing terminated employees' access to Delphi.

Delphi Security Requirements Not Enforced

Agencies are required to perform periodic Certification and Accreditation (C&A) reviews to determine whether a computer system is adequately secured commensurate with the associated risks. The C&A review starts with a risk-based security plan detailing security requirements needed for the system. While such a plan has been developed for Delphi, we found that the following requirements in the Delphi security plan are not enforced.

- Protecting sensitive information. We found that access to the Social Security Numbers and purchase credit card information was not restricted to people who had a legitimate need to know. Over 35,000 employees' Social Security Numbers and 678 Government-issued purchase card numbers are stored in Delphi for the expense reimbursement process. Currently, over 400 Delphi users can view all DOT employees' Social Security Numbers stored in the system. This not only reduces employee privacy but also increases the risk of identity theft. Unless corrective action is taken, the magnitude of this exposure will increase significantly as a result of FAA's conversion to Delphi, which will more than double the volume of sensitive information.

  In addition, while most Delphi information is encrypted during transmission, we found incidents where employee Social Security Numbers and purchase card information were transmitted over DOT networks in clear text and, if intercepted, could easily be copied.

- Ensuring integrity of system interfaces. Delphi interfaces with over 30 feeder systems, which provide Delphi with detailed financial data such as payroll expenses or grant obligations. These interfaces account for $42 billion in financial processing each year. A key security requirement for Delphi is that these feeder systems provide evidence of adequate security in the form of C&A documentation. C&A reviews are used to determine whether the system is adequately secured. In addition, the owner of each system interfacing with Delphi is required to sign a memorandum of agreement specifically documenting that their system is secure.

  These requirements are critical to ensure Delphi's own processing integrity. For example, in an August 30, 2002 memorandum, Delphi management stated that any feeder system not complying with these security requirements would be disconnected from Delphi. To verify compliance with this requirement, we judgmentally selected eight major interfacing systems for review. We found that three of eight feeder systems did not have any evidence of adequate security. Equally important, there is no action plan to ensure that these three systems obtain such evidence in a timely manner to continue their interfaces with Delphi. While the other five had such evidence, only one provided it to Delphi management. DOT management needs to obtain security evidence from feeder systems or disconnect their interface with Delphi by October 31, 2003.

- Enforcing personnel accountability. Delphi's security plan requires that employees and contractor personnel accept security responsibilities (rules of behavior) before being given access to Delphi. These rules of behavior inform users of their security responsibilities such as non-disclosure of passwords and proper handling of sensitive information. Rules of behavior also serve as a contract allowing management to hold users accountable in case of a security breach.

  We judgmentally selected 14 users from the Federal Transit Administration and the Federal Railroad Administration for review. We found that four of seven transit employees and all seven railroad employees had not signed rules of behavior. We further found that the railroad security administrator was not even aware of this security requirement.

- Conducting background checks. Background checks are key to ensuring adequate personnel security. While background checks provide no guarantee of a person's loyalty or trustworthiness, they provide valuable information that might keep at-risk personnel from working on Delphi. DOT policy[5] requires

[5] DOT Order 1630.2B, entitled "Personnel Security Management," dated May 30, 2001.

that key computer positions, such as network administrators, be designated as high risk and receive a higher level background check, called Background Investigation.

We judgmentally selected 14 individuals occupying sensitive positions, including network and database administrators, and found as shown in the table below, that 8 (about 57 percent) employees and contractor personnel did not receive Background Investigations.

Background Checks on Sensitive Positions

Sensitive Positions	Total Employees Tested		Employees Needing a Background Investigation	
	Federal	Contractor	Federal	Contractor
Network Administrators	1	6	1	2
System Programmers	0	5	0	3
Database Administrators	1	0	1	0
Security Officer	1	0	1	0
Totals	3	11	3	5
	14		8	

These individuals served as the first line of defense for Delphi security. For example, network administrators are responsible for network firewall security. System programmers essentially controlled all aspects of Delphi system operations. However, they did not receive proper background checks commensurate with the sensitivity of their positions.

These deficiencies existed because the Delphi security administrator did not enforce security requirements. The administrator was four levels below the Director of Delphi operations at the Aeronautical Center, and was focused on detailed administrative work such as processing user access requests.

To help with the duties of security administration, DOT has now appointed a Delphi information system security officer who will report to a higher level of authority. However, DOT management needs to continue implementing security controls necessary in Delphi, such as using secure mechanisms to transmit sensitive information, protecting employee Social Security Numbers stored in Delphi, obtaining DOT and contractor employees' signatures on the rules of behavior, and completing proper background checks on personnel occupying sensitive positions.

RECOMMENDATIONS

We recommend that the Acting Assistant Secretary for Budget and Programs/Chief Financial Officer direct the Office of Financial Management to:

1. Enhance basic system controls such as establishing password configuration controls, disconnecting users for inactivity during Delphi computer sessions, disabling user accounts not used over a specified time period, and systematically removing terminated employees' access to Delphi.

2. Restrict access to employee Social Security Numbers and purchase card information stored in Delphi to people with a legitimate need to know, and use secure mechanisms to transmit sensitive information on DOT networks.

3. Obtain evidence that all Delphi feeder systems are adequately secured from their system owners, or disconnect their interfaces by October 31, 2003.

4. Obtain signed rules of behavior documents from all Delphi users, or terminate their access by September 30, 2003.

5. Complete Background Investigations on the eight employees we identified.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

DOT has completed action on recommendation 4, and expects to complete action on recommendations 1, 2, 3, and 5 by December 2003. The actions taken and in process are responsive to the recommendations.

D. System Changes Need to Be Better Controlled

While the Delphi team used a structured process to control system changes, we found that change controls were not adequate in Delphi. Specifically, we found that testing was inappropriately performed on the production machine, key personnel were not involved in reviewing test results from system changes, and testing documents were not retained for future reference. As a result, DOT has limited assurance that only authorized changes were made to the system.

Testing Work Performed on the Production Machine

System changes should be made, tested, and reviewed in a test environment, and only approved changes should be accepted into production. While Delphi system support staff performed detailed testing on a test machine, we found that they conducted quality assurance testing and stress testing on the production machine. Problems experienced during testing could have an adverse impact on the Delphi production machine. For example, stress testing could cause the production system to experience performance degradation or a system crash.

Also, to ensure that only approved changes are implemented in production, system development staff responsible for making program changes should not be allowed to access the production machine. By allowing system development staff to perform testing work on the production machine, management had limited assurance that only authorized program changes were made.

Key Personnel Not Involved in the Change Control Process

An important principle in change control is ensuring that end-user needs are appropriately addressed when making changes to the system. Delphi had a Change Control Board (the Board) responsible for approving and prioritizing change requests, and assigning personnel to review test results. However, the Board was composed of only system development personnel at the Aeronautical Center without any OA user representation. As a result, DOT has limited assurance that changes requested by users are adequately considered for Delphi. OA managers also expressed concerns that OAs were not being represented on the Board and that their changes were not given sufficient priority.

Also, the Delphi security administrator was not involved in the change control process. As a result, there was little assurance that Delphi security would not be impacted during the change. For example, in one instance, password controls were set to a lower level on the test machine to facilitate program changes during an upgrade in October 2001. However, the controls were not reset to an acceptable level before the upgrade was installed on the production machine. The

lower level of Delphi security controls was not detected for over 1 year, until pointed out during our audit.

Testing Documents Not Retained

We judgmentally selected 10 System Change Requests completed in the past 1-year period and reviewed the documentation supporting the modification and testing process. While there was evidence of Board review and sign-off on system changes, we found that test plans and results were not retained for these requests.

Delphi management explained that the test plans and results were destroyed because of limited file storage space. Delphi management relied on approvals recorded in the tracking system as evidence of adequate testing. However, without these records, the Delphi team might experience additional difficulties when researching future system problems. DOT needs to ensure that test documents supporting critical changes are retained.

As a result of our audit, DOT management has removed the test database from the Delphi production machine. However, continued management attention is needed to have OAs represented on the Change Control Board for reviewing Delphi change requests and test results, require the security administrator to ensure that security is not degraded during system changes, and develop a policy for retaining system change documents based on the criticality of the change.

RECOMMENDATIONS

We recommend that the Acting Assistant Secretary for Budget and Programs/Chief Financial Officer direct the Office of Financial Management to:

1. Include key personnel, such as the security administrator and OA user representatives, on the Delphi Change Control Board to review and prioritize change requests.

2. Issue guidance for retaining test plans and results of system changes based on the criticality of the change.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

DOT has completed action on recommendation 1 and expects to complete action on recommendation 2 by December 2003. The actions taken and in process are responsive to the recommendations.

E. Contingency Plans Need to Be Enhanced and Tested

We found that the April 2001 contingency plan for Delphi was not adequate to ensure timely restoration of services for continued operations. Also, Delphi operations were vulnerable to telecommunications service disruptions at the Aeronautical Center. As a result, should Delphi operations experience service disruptions, it was unclear when the operation could be restored.

DOT Order H1350.254, entitled "Guide to Continuity of Operations Planning," requires OAs to restore critical DOT operations in case of a disruption of services. However, the Delphi contingency plan was not adequate to ensure continued payment and accounting operations at DOT. The plan called for use of on-site portable trailers containing computer hardware and electrical generators. This plan was not adequate in case of a major catastrophe at the Aeronautical Center because it would not be able to provide support, such as telecommunications, to these trailers. The plan should have included an off-site facility that provides for computer and telecommunications equipment necessary for a quick recovery of Delphi services.

We also found that the Aeronautical Center is at risk of losing all telecommunications lines, which would render Delphi inoperable. While these major telecommunications lines used different entry points into the Aeronautical Center, they converged in one room before entering the data center. If a failure occurred in this room, such as a fire, all telecommunications to the data center would be lost. Consequently, OA users would not be able to access Delphi to process payment requests or record accounting transactions.

During our audit, DOT management revised the Delphi contingency plan by selecting an off-site facility for recovery processing. DOT performed limited off-site tests on July 27 and September 7, 2003. However, management needs to develop a plan to eliminate converging major telecommunications lines in a single room at the Aeronautical Center.

RECOMMENDATIONS

We recommend that the Acting Assistant Secretary for Budget and Programs/Chief Financial Officer direct the Office of Financial Management to:

1. Conduct a comprehensive system recovery test by September 30, 2003.

2. Develop and implement a plan to eliminate converging major telecommunications lines in a single room at the Aeronautical Center.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

DOT has completed action on both recommendations 1 and 2. The actions taken are responsive to the recommendations.

ACTION REQUIRED

Actions taken and planned by DOT are reasonable. These issues are resolved, subject to the follow-up requirements in DOT Order 8000.1C. Therefore, no further response is required.

We appreciate the courtesies and cooperation of DOT and the Operating Administrations' representatives. If you have questions concerning this report, please call me at (202) 366-1992 or Ted Alves, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

#

EXHIBIT A. SCOPE AND METHODOLOGY

We used the General Accounting Office's Federal Information Systems Controls Audit Manual as a guide for this audit. Our review covered 12 DOT organizations using Delphi during our audit period.

We reviewed and analyzed Delphi's security plan, system change control procedures, interface control process, web configuration, firewall security rules, and contingency plan. We performed detailed analysis of system access privileges assigned to about 1,500 users, including system support personnel and OA users. We physically inspected environmental control systems such as fire extinguishers, physical access controls, backup power systems, and the backup file storage site.

We performed hands-on testing of Delphi password security and protection of sensitive information. We also judgmentally selected 10 system change requests, 14 personnel background checks, and 14 users' acceptance of security responsibilities for detailed review. We conducted interviews with key Delphi support personnel at the Aeronautical Center and OA users at DOT Headquarters.

In addition, we used various automated tools to test Delphi web and network security. By using commercial scanning software, we performed a vulnerability assessment on Delphi web sites, firewall security, and selected computers. We also used an automated tool to identify unauthorized telephone line connections (dial-up modem) to the Aeronautical Center networks. After identifying these dial-up modems, we made a manual effort to connect to them from outside of DOT and verified if these modems used password authentication or a call-back mechanism.

Our audit work was performed between November 2002 and July 2003 at FAA's Mike Monroney Aeronautical Center at Oklahoma City, Oklahoma, and DOT Headquarters in Washington, D.C. The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

THE FOLLOWING INDIVIDUALS CONTRIBUTED TO THIS REPORT.

Name	Title
Phil deGonzague	Project Manager
Ping Sun	Senior Computer Scientist
James Mallow	Senior Auditor
Henry Lee	Computer Scientist
Brad Kistler	Information Technology Specialist
Jean Ablutz	Information Technology Specialist

APPENDIX. MANAGEMENT COMMENTS

September 12, 2003

MEMORANDUM TO: Theodore P. Alves
Assistant Inspector General for
Financial and Information Technology Audits

Rebecca C. Leng
Deputy Assistant Inspector General for
Information Technology and Computer Security

(original signed by A. Thomas Park)

FROM: *for* Phyllis F. Scheinberg
Acting Assistant Secretary for Budget and
Programs/Chief Financial Officer

SUBJECT: Draft Report on Computer Security and Controls
Of Delphi Financial Management System,
DOT Project Number 03F3002F0000

Thank you for the draft report of your audit on computer security and controls for Delphi, the new financial management system that DOT is currently implementing. We appreciate the help your staff provided in identifying computer security and control issues so that we can ensure that Delphi fully implements and maintains effective security and controls.

We have worked closely with your staff during the review and as you noted in your report, as soon as issues have been raised we have taken immediate action to mitigate risks and to strengthen Delphi security and controls. Major corrective actions we have taken to enhance Delphi security and controls in response to your audit include:

- Implemented a Disaster Recovery site at the Federal Aviation Administration (FAA) Great Lakes Regional Office and conducted two successful disaster recovery tests with your staff's participation.

- Developed and implemented a Compatibility Matrix to ensure appropriate Separation of Duties for all Roles and Responsibilities assigned to Delphi users.

- Established and automated Rules of Behavior as part of the Delphi sign-in script.

- Reduced the number of users with system access and with physical access to the Systems Maintenance Facility, the data center at the Mike Monroney Aeronautical Center.

- Reviewed and eliminated all Web vulnerabilities.

- Submitted requests for upgrading the background level investigations for the remaining Delphi system administrators.

- Established the Delphi Management Committee composed of representatives from the Operating Administrations (OAs) to guide operations and enhancements to the system.

- Enhanced the System Change Request process to provide the OAs with greater input on proposed system enhancements and the priorities for accomplishing them.

Attached is a spreadsheet that provides more details on all the corrective actions we are taking and have completed to address the recommendations in your draft audit report.

The *Oracle Federal Financials* software used by Delphi provides extensive security features and controls, as described by Oracle security experts who met with your staff earlier this year. We are working with the Chief Information Officer's staff to renew the Certification and Accreditation of Delphi and to ensure that all feeder systems have been properly Certified and Accredited.

We look forward to continuing to work with your staff to enhance Delphi security and controls further as the system continues to evolve beyond the implementation phase. Please refer any questions to Larry Neff of the DOT Office of Financial Management at (202) 366-2335.

Attachment[1]

cc:
Dan Matthews
Lisa Schlosser
Lindy Ritz
Robert Stevens
Keith Burlison
Keith Nelson
Cheryl Rogers
Laura Ramoly
Mike Myers
A. Thomas Park
Larry Neff
Kean Miller

[1] For security reasons, the Attachment, which provided specifics on DOT's corrective actions, is not included in this report.

APPENDIX. MANAGEMENT COMMENTS