# Memorandum

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

Subject: ACTION: Quality Control Review of the Report on Controls Over the Enterprise Service Center's Delphi Financial Management System Report No. QC-2006-076

Date: September 29, 2006

From: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

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

This report summarizes the results of the review of system security controls over the Department of Transportation (DOT) Enterprise Service Center's (ESC) Delphi Financial Management System. The ESC performs accounting and financial management functions for DOT and other Federal organizations. It is maintained by Federal Aviation Administration employees at the Mike Monroney Aeronautical Center in Oklahoma City.

ESC is one of four Centers of Excellence designated by the Office of Management and Budget to provide financial management information system services to other governmental agencies. ESC supports other Federal entities, the National Endowment for the Arts, and the Institute of Museum and Library Services. The Office of Management and Budget requires Centers of Excellence to provide client agencies with an independent audit report in accordance with the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards.

This year's audit was completed by Clifton Gunderson, LLP, of Calverton, Maryland. We performed a quality control review of the audit work to ensure that it complied with applicable standards. These standards include the Generally Accepted Government Auditing Standards and AICPA's Statement on Auditing Standards (SAS) 70. In our opinion, Gunderson's audit work complied with applicable standards.

The Clifton Gunderson audit report concluded that management's description of controls for the Delphi Financial Management System presents fairly, in all material respects, the controls that had been placed in operation as of May 31, 2006. In addition, on 9 out of 10 control objectives, the independent auditor concluded that controls, as described, are suitably designed and were operating effectively during the period from October 1, 2005, through May 31, 2006. This represents a significant improvement from last year and is the result of a concerted effort made by DOT Headquarters staff and ESC management to implement previous audit recommendations.[1]

This enhanced operational environment enabled auditors to rely on Delphi Financial Management System controls when conducting this year's financial statement audits. However, continued improvement is needed. Specifically, Gunderson reported that controls were not suitably designed and not operating with sufficient effectiveness to achieve one stated objective, "Logical Access Controls provide reasonable assurance that safeguards are established to prevent or detect unauthorized access."[2]

- Not Suitably Designed. The computer network architecture was not suitably designed to provide adequate logical access controls. Delphi system servers reside in a network that is shared by all users at FAA's Mike Monroney Aeronautical Center. The ESC staff responsible for maintaining Delphi does not fully control this shared network. If the network is not properly secured, other systems on this network could become an entry point of unauthorized access to the Delphi Financial Management System. Management should install firewall protection to limit access to Delphi servers by other Aeronautical Center system users.

- Not Operating Effectively. Controls were not operating with sufficient effectiveness in the areas of programmer access to production servers, timely revocation of terminated employees' system access, and network equipment vulnerability to known security risks. ESC management needs to enforce better control practices.

Gunderson made 12 recommendations to improve controls and submitted them to DOT management. We agree that implementing these recommendations would further enhance controls over Delphi Financial Management System operations and have included these recommendations in this report (see Exhibit). In a September 26, 2006, response to the Office of Inspector General, the DOT Deputy

---

[1] Report Number QC-2005-075, "Quality Control Review of the Report on Controls over the Delphi Financial Management System," September 2, 2005. In this report, auditors concluded that controls were suitably designed for 8, and operating effectively for 7, of the 10 stated control objectives. OIG reports can be found on our website: www.oig.dot.gov.

[2] The independent auditor's report is available upon request.

Chief Financial Officer concurred with the recommendations and committed to implementing corrective actions (see Appendix).

In accordance with DOT Order 8000.1C, the corrective actions taken in response to Gunderson's recommendations are subject to audit follow-up. Gunderson is performing additional testing and will prepare a follow-up management letter to the Office of Inspector General reporting whether the control environment changed significantly between June 1 and September 30, 2006. After receiving Gunderson's follow-up letter, we will decide whether additional support, including target completion dates, is needed for the corrective actions.

We appreciate the courtesies and cooperation of ESC, the Office of the Secretary of Transportation, and Clifton Gunderson representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1496 or Edward Densmore, Program Director, at (202) 366-4350.

Attachments

#

cc: Chief Information Officer, Department of Transportation
Federal Aviation Administrator
Assistant Administrator for Financial Services/CFO, FAA
Assistant Administrator for Information Services/CIO, FAA
Assistant Administrator for Region/Center Operations, FAA
Director, Mike Monroney Aeronautical Center, FAA
Martin Gertel, M-1
Anthony Williams, ABU-100

## EXHIBIT. RECOMMENDATIONS OF CLIFTON GUNDERSON, LLP, INDEPENDENT AUDITOR

**DOT Management should implement the following actions to enhance Delphi security administration controls.**

1. Division/Administrative Heads and Departmental COTRs should notify the Delphi ISSO of all new hires and request that the ISSO provide justification that all new system users have received the requisite security training within the mandated 30 day period. These management personnel should ensure strict adherence to existing DOT policies with respect to documenting the new employee/contractor checklist; routing all new hire information via Human Resources to the Delphi ISSO so that mandatory security training can be enforced.

2. Ensure the Delphi Incident Response Capability includes all requirements as stipulated by the National Institute of Standards and Technology – Special Publication 800-61 – "Computer Security Incident Handling Guide".

**DOT Management should implement the following actions to enhance Delphi physical access controls.**

3. Perform an analysis of all employees with access to the data center and document the motive for this access. Periodically review this list and have the system owners certify their users. Review access frequency and remove permanent access for employees who do not need this access in the daily execution of their duties.

4. Develop and implement log review policies to ensure the visitor log is filled out in its entirety each time a person visits the data center. Ensure punitive measures are implemented against employees (escorts) who do not abide by these policies.

5. Install Closed Circuit TV cameras.

**DOT Management should implement the following actions to enhance Delphi backup, recovery, and maintenance controls.**

6. ESC Management should periodically test the SMF Disaster Recovery plan.

**DOT Management should implement the following actions to enhance Delphi logical access controls.**

7. ESC Management should consider implementing a security enclave that would separate the Delphi servers by placing the servers on their own internal IP network. The access to this network should be controlled by firewalls and monitored by IDS. In the short run, coordinate patch management and other security features for all agencies that own hardware/software in the MMAC data center.

8. ESC Management should review the current rights of programmers and remediate inappropriate access.

9. Management should review the automated process for revoking access to operating system accounts. Review the current process and refine the method of disabling and/or removal of access accounts at the application and operating system levels.

10. Conduct network (Internal and External) scans periodically including scans of System Administrator workstations and terminals. Alternate or rotate scanning software as different tools depending on their settings will capture vulnerabilities differently.

**DOT Management should implement the following actions to enhance Delphi application input controls.**

11. In addition to the quarterly recertification of user access, we recommend Delphi management team strengthens its monitoring techniques over powerful application privileges.

12. We recommend that all Delphi users' access be reviewed on a quarterly basis to ensure their rights and privileges are based on a need-to-know principle. ESC should enforce this policy for all Delphi Customers. Also, ESC should immediately revoke a users' access when such revocation is requested by the user's Security Officer.

## APPENDIX. MANAGEMENT COMMENTS

September 26, 2006

MEMORANDUM TO: Rebecca C. Leng
Assistant Inspector General for Financial, Information Technology, and Departmentwide Programs

FROM: Larry Neff
Deputy Chief Financial Officer

SUBJECT: Management Response to Security Audit of the Delphi Financial Management System

Thank you for the Quality Control Review report of the Delphi Financial Management System, which is operated and maintained for the Department of Transportation by the Enterprise Services Center (ESC) in Oklahoma City. We appreciate all the help the Office of Inspector General (OIG) staff provided in coordinating Clifton-Gunderson's Statement on Auditing Standards (SAS) 70 audit of Delphi for Fiscal Year 2006.

We have worked closely with the auditors throughout this SAS-70 review to ensure that as soon as an issue was raised, immediate action was taken to mitigate risks and to further strengthen Delphi's security controls. Corrective actions taken to enhance Delphi's security controls in response to this year's SAS-70 audit include:

- Security Awareness Training procedures for the Office of Enterprise Systems (AME) have been enhanced and management has been informed of the new procedures.
- The Delphi Incident Response Plan has been updated to include all elements as described in NIST 800-61, and the updated plan has been distributed to all Delphi personnel.
- The procedures for handling visitors to the Systems Maintenance Facility (SMF) data center have been enhanced. Visitors to the SMF are now issued Visitor Badges on entering the SMF. These procedures also include updating the SMF Visitor Log.
- The SMF Disaster Recovery Plan has been updated and tested, and the test results have been documented.

- Documentation of SMF Tape Restoration procedures has been completed.
- Production and Development Operating System (OS) accounts have been updated to ensure access is limited based on business need.
- OS Account Revocation procedures have been enhanced.
- All unpatched software has been removed from System Administrators' workstations.
- Delphi support staff production update responsibilities have been reviewed to ensure all are appropriately end-dated.
- The Delphi User Recertification process has been enhanced and communicated to the Delphi Security Officers.
- All "Null" sessions have been disabled.
- The ISCS has implemented a monthly scan of all Delphi System Administrator, Application Administrator, and Database Administrator workstations.
- Any available and required server patches have been applied.
- Delphi Windows-based servers have had Host-Based firewalls installed.
- All high internal scan findings have been mitigated.

**The following additional corrective actions are currently underway:**

- The SMF is in the process of researching other methods to enforce visitor sign-in and sign-out.
- Cameras are scheduled to be installed in the SMF as part of the ongoing Aeronautical Center-wide Facility Security Risk Management (FSRM) Project. The cameras will provide surveillance and recording capability for activity within the SMF. The FSRM project's installation, test and commissioning phases are scheduled for December 2006 through May 2008.
- Delphi Windows Servers are scheduled to have Host-Based firewalls installed by December 15, 2006.
- An Access Portal is scheduled to be implemented for access to Delphi applications by December 31, 2007, or earlier if possible, depending on the schedule for the upgrade to release 11.5.10 of the *Oracle 11i e-Business Suite*. Once implemented, users will only be able to view information on the site after authentication. In addition, research is currently underway to determine if the Delphi Internet Home Page (idelphi) can be disabled.

## APPENDIX Management Comments

We look forward to continuing to work with you and your staff to strengthen the design and implementation of Delphi security controls. As a Shared Service Provider (SSP) designated by the Office of Management and Budget (OMB) to provide other Federal agencies with our Delphi financial system and accounting services, we are strongly committed to ensuring that the Delphi Financial Management System meets or exceeds all security requirements.

Thank you for your continuing support and assistance in this effort.

Attachment

cc:
Joann Adam, Lindy Ritz, Stan Sieg, Marshal Gimpel, Bob Stevens, Keith Burlison, Cheryl Rogers, Mike Myers, Laura Ramoly, Phil Loranger, Laurie Howard, Joanne Choi, Sheldon Edner, Arvid Knutsen

## FY 2006 Delphi SAS-70 NFR Action Plan Summary as of September 26, 2006

| NFR # | Description | Status | Corrective Actions |
|---|---|---|---|
| 1.1 | AME Security Awareness Training | Completed | ▪ Create Security Awareness Training Procedures<br>▪ Inform AME Management of Training Procedures |
| 1.2 | Delphi Incident Response Plan | Completed | ▪ Update Delphi Incident Response Plan<br>▪ Internal Management Review of updated Plan<br>▪ Distribute updated Plan to Delphi personnel |
| 2.1 | SMF Physical Access | Completed | ▪ Enhance access procedures |
| 2.2 | SMF Visitor Log | In Progress | ▪ Procure SMF Visitor Badges<br>▪ Implement ID/Badge Swap-Out |
| 2.3 | SMF Cameras | In Progress | ▪ Install Cameras in the SMF |
| 3.1 | Test of SMF Disaster Recovery Plan | Completed | ▪ Document SMF DR Test Results |
| 3.2 | SMF Tape Restoration Procedures | Completed | ▪ Document Tape Restoration Procedures |
| 4.1 | Network Logical Access Controls | In Progress | ▪ Install Host-Based Firewalls on Windows servers |
| 4.2 | DEV and PROD OS Accounts | Completed | ▪ Remove OS Access for 3 Programmers<br>▪ Research OS Access of DBA<br>▪ If necessary, remove OS Access of DBA |
| 4.3 | OS Account Revocation Process | Completed | ▪ Enhance OS Account Revocation Process |
| 4.4 | Website Info Prior to Logon | In Progress | ▪ Implement Portal for Access to all Delphi Apps/Info |
| 4.5 | NULL Sessions | Completed | ▪ Research Need for NULL Sessions<br>▪ If feasible, disable NULL Sessions |
| 4.6 | Compromised Workstation | Completed | ▪ Remove Unpatched Software<br>▪ Create Process to Scan SA/DBA/AA Workstations |
| 4.7 | Penetration Test Findings | Completed | ▪ Research/Apply Servers Patches, as Appropriate |
| 4.8 | Internal Scan Findings | Completed | ▪ Mitigate Internal Scan Findings |
| 5.1 | Open/Close Responsibilities | Completed | ▪ End-Date GL Access Responsibilities |
| 5.2 | Delphi User Recertification | Completed | ▪ Enhance/Enforce User Recertification Process |