# 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 Delphi Financial Management System, DOT
QC-2005-075

Date: September 2, 2005

From: Theodore P. Alves
Principal Assistant Inspector General
for Auditing and Evaluation

Reply to Attn. of: JA-20

To: Phyllis F. Scheinberg
Assistant Secretary for Budget and Programs and 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 (service center) Delphi Financial Management System. The Delphi Financial Management System performs accounting and financial management functions for DOT and other Federal agencies. It is maintained by Federal Aviation Administration employees at the Mike Monroney Aeronautical Center in Oklahoma City, Oklahoma, under the direction of the departmental Chief Financial Officer.

The service center is one of four Centers of Excellence designated by the Office of Management and Budget (OMB) to provide financial management information system services to other Federal agencies. To date, the service center supports one other Federal agency, the National Endowment for the Arts. OMB requires Centers of Excellence to provide Federal agencies with an independent audit report in accordance with the American Institute of Certified Public Accountants (AICPA) standards.

Clifton Gunderson, LLP, an independent auditor, of Calverton, Maryland, completed the review. The Office of Inspector General (OIG) performed a quality control review of Gunderson's audit work to ensure that it complied with applicable auditing standards Generally Accepted Government Auditing Standards and the AICPA's Statement on Auditing Standards (SAS) 70. In our opinion, Gunderson's audit work complied with applicable standards.

The 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, 2005. In addition, Gunderson concluded that controls, as described, are suitably designed to provide reasonable assurance that 8 of the 10 specified control objectives would be achieved, if these controls were complied satisfactorily. Gunderson's testing found that controls were operating effectively to provide reasonable assurance that 7 of the 10 control objectives were achieved during the period from October 1, 2004 to May 31, 2005.

We agree with Gunderson that strengthening the design and operational effectiveness in these control objective areas will further enhance Delphi Financial Management System operations. However, the service center and DOT Headquarters management deserve credit for making a concerted effort to enhance security and controls over Delphi system operations, as recommended in OIG's September 2003 report. [1]

Specifically, since September 2003, DOT management implemented more disciplined security administration and oversight of Delphi operations, strengthened controls over access to the General Ledger module to ensure the integrity of financial statement compilation in Delphi, and installed an enclosed area in the computer center to better protect Delphi servers. In addition, management enhanced controls over changes to Delphi production programs and tested the contingency plan to ensure continuity of Delphi operations in case of emergency.

Gunderson reported that controls were not suitably designed or not operating effectively from October 1, 2004 to May 31, 2005 for the following control objectives.

- **Security Administration Controls**. Gunderson concluded that controls described are suitably designed; however, they were not operating effectively in several areas. Specifically, the service center did not update the security plan to reflect the operating system upgrades in Delphi and enhanced security protection of Delphi servers in the computer center; security accreditation for three interfacing systems had expired and need to be re-certified; the memorandum of understanding was not provided for a National Endowment for the Arts interfacing system, as required; and management did not provide alternative training measures when the security awareness website was not functional.
- **Logical Access Controls**. Gunderson concluded that the control used to capture incompatible duties/roles for Delphi processing was not suitably

[1] Report Number FI-2003-094, "Report on Computer Security of Delphi Financial Management System," September 30, 2003. OIG reports can be found on our website: www.oig.dot.gov.

designed because it is a detective control rather than a preventive control. Gunderson also concluded that described controls were not operating effectively in the areas of separating incompatible duties and restricting access to the operating system software on the Delphi computer server.

- **Physical Access Controls**. Gunderson concluded that the control used to grant access to the computer center, which houses Delphi and other computer systems, was not suitably designed because it does not ensure that access is granted in accordance with an individual's job function/responsibilities. Gunderson also concluded that described controls were not operating effectively because an excessive number of people were granted access to the computer center, and management did not always specify justification for granting individuals' access to the computer center on the request form.

Gunderson made 12 recommendations to improve controls and submitted the recommendations to DOT management under separate cover from its report.[2] We agree that implementing these recommendations will further enhance controls over Delphi Financial Management System operations and have included these recommendations in this report (see Exhibit A). In an August 25, 2005, response to OIG, the DOT Deputy Chief Financial Officer concurred with the recommendations and committed to implementing corrective actions (see Appendix I).

In accordance with DOT Order 8000.1C, the corrective actions taken in response to Gunderson's recommendations are subject to follow-up. Gunderson is performing additional testing and will prepare a follow-up management letter to OIG by September 30, 2005, reporting whether the control environment has significantly changed between June 1 and September 30, 2005. 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 the Enterprise Service Center, 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) 366-1992, or Rebecca Leng, Deputy Assistant Inspector General for Information Technology and Computer Security, at (202) 366-1488.

Attachment

cc: Chief Information Officer, DOT
Federal Aviation Administrator

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

# EXHIBIT A. CLIFTON GUNDERSON, INDEPENDENT AUDITOR, RECOMMENDATIONS

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

1. Ensure all systems that connect to the Delphi are certified and accredited and have established interconnection agreements.

2. Update the computer center (SMF) Security Plan to reflect changes in the facility.

3. Implement measures to ensure employee awareness training is always available.

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

4. Accelerate the implementation of “Sox Out of the Box” access control software to provide preventive security controls to separate incompatible duties and roles for Delphi processing.

5. Ensure that representatives from the National Endowment for the Arts sign a liability waiver for noncompliance with ESC’s recommended security parameters on assigning roles and responsibilities to Delphi users.

6. Restrict access to the audit log repository to only those individuals with security and review responsibilities.

7. Review who has access to high “root-level” access to the Delphi operating system and formally document the authorization for granting access to legitimate users. Provide adequate training on this privileged account before granting access.

8. Reduce the number of users with “root-level” access to the Delphi operating system. Deactivate the “root-level” access assigned to one terminated employee.

9. Review the Delphi operating system settings on a periodic basis and notify the SMF (Information System Security Officer (ISSO) of all discrepancies for immediate action.

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

10. Reduce the number of employees and contractors with access to the SMF computer center and complete the transfer of all Delphi servers into the caged area.

11. Require division managers with employees and contractors requiring access to the SMF computer center to:
    - Properly document the justification for physical access requests to SMF.
    - Review monthly the list of employees and contractors who have access to the SMF.
    - Perform a quarterly recertification of authorized user access to the facility.

12. Explore the feasibility of implementing a biometric key card for physical access to the SMF computer center that expires every 90 days and triggers a need for quarterly recertification.

# APPENDIX I. MANAGEMENT COMMENTS

# Memorandum

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

Subject: Management Response to the Quality Control Review of the Enterprise Service Center's Delphi Financial Management System

Date: August 25, 2005

From: Lawrence I. Neff
Deputy Chief Financial Officer

Reply to Attn. of: B-2

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

Thank you for the Enterprise Service Center (ESC) Quality Control Review report of the Delphi Financial Management System. We appreciate all the help the Office of Inspector General (OIG) staff provided in coordinating Clifton-Gunderson's Statement on Auditing Standards (SAS) audit of Delphi.

We have worked closely with the auditors throughout the SAS-70 review. As issues were raised, immediate actions were taken to mitigate risks and to further strengthen Delphi's security controls. Corrective actions taken to enhance Delphi security controls in response to this SAS-70 review include:

- Interconnection agreements for all Delphi interfaces have been completed.
- The ESC computer center (SMF) Security Plan has been updated to reflect changes in the facility, such as the OIG-recommended server isolation cage.
- Agency-specific Security Awareness training is now available online, with CD-ROM based training being available for sign-out locally. In addition, in-processing procedures have been updated to ensure all new employees receive Security Awareness training within 30 days of starting work.
- Per the auditor's recommendation, the National Endowment for the Arts (NEA) submitted and the Delphi System Owner approved a time-limited Incompatible Roles Risk Acceptance, pending the implementation of the *SOX Out of the Box* software this Fiscal Year.
- Individuals with system Root Access privileges have had their access reviewed and their authorization formally documented. System Administrators receive specialized, supervised training prior to being granted elevated privileges.
- We are continuing to reduce the number of individuals with access to the SMF computer center. In addition, all Delphi servers have been relocated to the further restricted locked caged area.

- The SMF computer center's process for authorizing physical access has been strengthened to ensure proper justifications for access exist and that access lists are recertified quarterly. In the future, as the Department implements the requirements of Homeland Security Presidential Directive 12 (HSPD 12), *Policy for a Common Identification Standard (CIS) for Federal Employees and Contractors*, more robust physical access measures may be incorporated.

The following additional corrective actions are currently underway:

- Two remaining Delphi interfacing systems do not have a current certifications & accreditations (C&A). One system, owned by B-30, is scheduled to sunset in the near future; therefore, the Delphi System Owner has accepted the risk of this system not being recertified. The other system's recertification is presently underway, with a scheduled completion date of September 30, 2005.

- The *SOX Out of the Box* application is on schedule to be implemented in the Delphi Production environment by the end of August. In testing, *SOX* has been successful at masking SSN numbers and in proactively enforcing the Delphi Incompatibility Matrix at the transaction level.

- Actions to restrict access to the Operating System Audit Log Repository are underway and are on schedule to be completed during August.

- By August 31, System Administrator Root Access on the Delphi production server will be further reduced by two individuals. Written approval from the DOT Deputy Chief Financial Officer (DFCO) will be required if these privileges should ever need to be reinstated. In addition, we are continuing to investigate the use of system utilities that could allow Administrators to maintain the system without using Root privileges.

Attached is a more detailed action plan that outlines specific actions that have been and are being taken to strengthen each security control discussed in the SAS-70 report.

We look forward to continuing to work with your staff to strengthen the design and implementation of Delphi security controls. As an Office of Management and Budget (OMB) designated Center of Excellence, we are strongly committed to ensuring the ESC's Delphi Financial Management System meets or exceeds all security requirements. Thank you for your continuing support and assistance in this effort.

Attachment

cc:
Dan Matthews, Darren Ash, Joanne Choi, Arvid Knutsen,
Lindy Ritz, Dick Rodine, Joanne Adam, Bob Stevens,
Cheryl Rogers, Keith Burlison, Mike Myers, Laura Ramoly