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-2007-072

Date: September 13, 2007

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. ESC performs accounting and financial management functions for DOT and other Federal organizations. The system is maintained by Federal Aviation Administration employees at the Mike Monroney Aeronautical Center in Oklahoma City, Oklahoma.

ESC is one of four Federal Service Providers designated by the Office of Management and Budget (OMB) to provide financial management information system services to other governmental agencies. In addition to serving DOT, ESC supports other Federal entities—the National Endowment for the Arts, Institute of Museum and Library Services, and the Commodity Futures Trading Commission.[1] OMB requires Federal Service Providers to obtain an independent audit in accordance with the American Institute of Certified Public Accountants' (AICPA) Statement of Auditing Standards.

This year's audit of the DOT ESC Delphi Financial Management System was completed by Clifton Gunderson, LLP, of Calverton, Maryland, under contract to the Office of Inspector General. 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

[1] The Government Accountability Office will be a new customer of the ESC beginning October 1, 2007.

Statement on Auditing Standards 70. In our opinion, Clifton 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, 2007. In addition, the independent auditor concluded that controls, as described, are suitably designed and were operating effectively from October 1, 2006, through May 31, 2007, for all stated control objectives except logical access control.[2]

Specifically, Clifton Gunderson found that management has not completed the planned corrective actions to provide reasonable assurance that safeguards for logical access controls have been established to prevent or detect unauthorized access.

- Logical Access Controls Were Not Suitably Designed. Last year, the auditors reported that computer network architecture and vulnerability assessment methodology were not suitably designed to provide adequate logical access controls.[3] Specifically, the Delphi database server resides in a shared network that is not fully controlled by ESC staff. Therefore, ESC's assessments could not ensure that all known vulnerabilities were identified and corrected. Management should implement protection mechanisms to limit access to Delphi servers by other Aeronautical Center system users. Otherwise, other systems on this network, if not properly secured, could become an entry point of unauthorized access to the Delphi Financial Management System.

  During fiscal year 2007, management made progress in isolating the Delphi Financial Management System servers and related resources on the network. However, the main Delphi servers are not scheduled to move into a better secured environment until May 2008.

- Logical Access Controls Were Not Operating Effectively. Logical access controls were not operating with sufficient effectiveness in the areas of vulnerability assessment, workstation administration, and intrusion detection and reporting. ESC management needs to enforce better control practices in these areas.

Gunderson made eight recommendations to DOT management for improving access controls. We agree that implementing these recommendations would further enhance controls over operations of the Delphi Financial Management

---

[2] The independent auditor's report is available upon request to current and prospective Delphi user organizations.

[3] "Quality Control Review of the Report on Controls over the Delphi Financial Management System," Report Number QC-2006-076, September 29, 2006. OIG reports can be found on our website: www.oig.dot.gov.

System. The recommendations are listed in the Exhibit to this report. In an August 30, 2007, response to the Office of Inspector General, the DOT Deputy 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 provide a follow-up management letter to the Office of Inspector General, reporting whether the control environment has changed significantly between June 1, 2007, and September 30, 2007. 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.

#

cc: Chief Information Officer, DOT
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

The following recommendations were made by Clifton Gunderson, LLP, in its 2007 independent auditor report on the DOT ESC Delphi Financial Management System. DOT Management should implement the following actions to enhance Delphi logical and physical access controls.

LOGICAL ACCESS	
1.	Ensure that the certification agent in the security certification and accreditation process of the Systems Maintenance Facility (SMF) general support system is an individual, group, or organization that retains an appropriate level of independence and remains free from conflicts of interest.
2.	Complete implementing the security enclave that would separate the Delphi servers by placing the servers on their own internal Internet Protocol network. Access to this network should be controlled by firewalls and monitored by intrusion-detection software. In the short run, coordinate patch management and other security features for all agencies that own hardware/software in the Mike Monroney Aeronautical Center data center.
3.	Follow DOT and FAA guidelines in determining the level of alerts to be reported to ESC. They should review the current alert thresholds set by the Computer Security Incident Response Center and ensure the IDS is configured based on the Internet Access Point Administrator's recommendations for the ESC's environment.
4.	Conduct network (internal and external) scans periodically, including scans of System Administrator workstations and terminals. To the extent possible, alternate or rotate scanning software and perform full scans at least quarterly or semi-annually, as resources may permit.
PHYSICAL ACCESS	
5.	Update SMF documentation to reflect the current responsible parties for administering the SMF.
6.	Perform fire drills so personnel are aware of physical security measures and exit procedures.
7.	Perform an analysis of all employees with access to the data center and document the justification for this access. Review access frequently and remove permanent access for employees who do not need this access in the daily execution of their duties.
8.	Review and assess management progress in implementing closed circuit TV cameras in the Multi-Purpose Building (housing the data center).

APPENDIX. MANAGEMENT COMMENTS

August 30, 2007

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

FROM: Lawrence I. Neff
Deputy Chief Financial Officer

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

Thank you for the Statement on Auditing Standards (SAS) 70 audit of the Department's Delphi Financial Management System, which is hosted and operated by the Enterprise Services Center (ESC) in Oklahoma City. We appreciate the Office of Inspector General's (OIG) coordination, oversight, and Quality Control Review of Clifton Gunderson's SAS-70 audit of Delphi.

We concur in the recommendations and have identified corrective actions to address them (copy attached). As in the past, we have worked closely with the auditors throughout this year's SAS-70 audit to ensure that as any issue was raised, corrective action was taken immediately to mitigate risks and to strengthen Delphi's security controls. Corrective actions already taken to enhance Delphi security in response to this year's SAS-70 audit include:

- We have implemented a quarterly full port scan of the Delphi servers. The first full port scan was conducted on June 23 and the next scan is scheduled for September 22. These full port scans are in addition to the many different vulnerability scans that are conducted each month as part of our standard operations, including: (1) twice weekly scans on the Demilitarized Zone (DMZ) hardware, (2) bi-weekly scans on all Delphi servers using Foundstone, and (3) quarterly scans on all Delphi servers using Nessus.

- All workstations used by Delphi System Administrators, Database Administrators and Application Administrators have had static IP addresses assigned. Vulnerability scans are performed quarterly to ensure that no inappropriate or unpatched software has been installed.

The following additional corrective action is currently underway:

- The majority of the Delphi servers have been moved to a separate IP address space (enclave) to facilitate external customer access to the Delphi System. We will move the Delphi production cluster to this enclave as well when we implement our next major hardware upgrade in May 2008.

Although the Delphi database server currently resides logically in a non-segmented network that is not fully controlled and managed by ESC personnel, this network is a trusted internal government network, which helps mitigate risks. The existing internal network architecture provides standard government IT security protection and controls, such as firewalls and Intrusion Detection Systems (IDS). In addition, the DOT and FAA IT security programs provide for Certification and Accreditation (C&A) of systems, rules of behavior, frequent vulnerability scanning, etc.

The same controls are applied to systems in the DMZ, which provides an additional layer of network-based firewall protection to segment the DMZ from the internal government network. These protective measures are consistent with industry best practices and comply with Federal, DOT and FAA security program requirements and guidance.

The ESC has been preparing for some time to upgrade the Delphi infrastructure and hardware to leverage newer, more cost-effective technologies. As part of this upgrade in May 2008, the newly-configured database cluster will be logically isolated to reside in a Virtual Local Area Network (VLAN) with restricted access.

We appreciate the help you and your staff have provided through the SAS-70 process as we have continued to strengthen the design and implementation of all security controls for Delphi every year, and we look forward to your continuing help and support.

As a Federal Shared Service Provider (FSSP) designated by the Office of Management and Budget (OMB) to provide a state-of-the-art financial system and quality accounting services to other Federal agencies, we are fully committed to ensuring that the Delphi Financial Management System meets or exceeds all information security requirements.

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

Attachment: Corrective Action Plan

cc:
Joann Adam, Phill Loranger, Laurie Howard, Wynne Davis, Hunter Phelps, Arvid Knutsen, Wendy Calvin, Lindy Ritz, Stan Sieg, Marshal Gimpel, Sara Smith, Keith Burlison, Sandra Schreiner, Jacque Estes, Cheryl Rogers, Mike Myers, Laura Ramoly, Robert Stevens

Attachment

Corrective Action Plan
For the FY 2007 SAS-70 Audit of Delphi

NFR #CO-2:

Recommendation 1*. We recommend that the ESC Management ensure that the Certifications Agent/s in the Security Certification and Accreditation process of the SMF general support system is an individual, group or organization that retain/s an appropriate level of independence and remain/s free from conflicts of interest.*

Management concurs with this recommendation. The ESC does assure that the SMF is certified by an independent organization that has no responsibilities for the development, maintenance, support or oversight of the systems they certify, as required by FISMA. To alleviate the appearance of any conflict of interest, per the signatures identified on the certification package reviewed by the auditors, ESC will coordinate a request to the ARC Information Systems Security Manager (ISSM) for appropriate changes to the template by September 28, 2007.

Recommendation 2. *ESC Management should complete implementing the security enclave that would separate the Delphi servers by placing the servers on their own internal IP network. 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.*

Management concurs with this recommendation. The majority of Delphi servers have already been moved to a separate IP address space (enclave) to facilitate external customer access to the Delphi System; the remaining servers will be moved to this enclave when the Delphi hardware is upgraded in May 2008. Combining completion of the security enclave with the hardware upgrade provides the greatest benefits for the costs required. Access to this enclave is initially being controlled utilizing Access Control Lists (ACLs). A determination on the addition of enclave firewalls, based on cost versus added security benefit, will be made by the Delphi Authorizing Official. In the interim, we will continue to coordinate patch management and other security features for all agencies that own hardware/software in the MMAC data center through our service provider agreements.

Recommendation 3. *ESC Management should follow DOT and FAA guidelines in determining the level of alerts to be reported to ESC. They should review the current alert thresholds set by CSIRC and ensure the IDS is configured based on the Internet Access Point Administrator's recommendations for the ESC's environment.*

Management concurs with this recommendation. ESC has controls in place, in accordance with DOT & FAA orders, to prevent unauthorized scanning and intrusion. Per FAA order1370.90, ESC perimeter routers limit CSIRC's view of the full impact of external scans; therefore, CSIRC would only see a small subset of the scanning activity performed for the SAS-70 audit, and because no improper access was attempted, this did not trigger any alerts (in addition, ESC ACLs are configured to block entire subnets known for inappropriate behavior). The MMAC Internet Access Point Administrator will review the current alert thresholds and ensure the IDS is correctly configured by August 17, 2007.

Recommendation 4. *Conduct network (Internal and External) scans periodically including scans of System Administrator workstations and terminals. To the extent possible, alternate or rotate scanning software and perform full scans at least quarterly or semi-annually as resources may permit.*

Management concurs with this recommendation. A quarterly full port scan, alternating scanning software, of Delphi servers has been implemented. The first scheduled full port scan was performed on June 23, 2007. The next scan is scheduled for September 22, 2007. These full port scans are in addition to the numerous vulnerability scans that are run throughout the month on DMZ hardware (twice weekly) and all Delphi servers (bi-weekly and quarterly scans utilizing alternate scanning software). In addition, all System Administrator, Database Administrator and Application Administrator workstations have had static IP addresses assigned, and vulnerability scans are performed quarterly to identify if inappropriate, unpatched software is installed. The most recent administrator workstation scan occurred on July 25, 2007.

NFR #CO-3:

Recommendation 1. *ESC Management should update SMF documentation to reflect the current responsible parties for administering the SMF.*

Management concurs with this recommendation. The SMF ISSP was updated in April 2007 as part of the SMF's annual FISMA Assessment. Appropriate SMF documentation will be updated in the future, as significant changes occur.

Appendix. Management Comments

Recommendation 2. *Fire drills should be performed so personnel are aware of physical security measures and exit procedures.*

Management concurs with this recommendation. The most recent fire drill was held on May 31, 2007. ESC will coordinate with MMAC Facility Maintenance to ensure routine fire drills are performed in a timely manner.

Recommendation 3. *Perform an analysis of all employees with access to the data center and document the motive for this access. Review access frequently and remove permanent access for employees who do not need this access in the daily execution of their duties.*

Management concurs with this recommendation. An analysis of employee access to the data center will be completed by August 31, 2007. In addition, regularly scheduled quarterly access reviews of employee access to the data center will continue. The next data center quarterly access review will be completed by September 30, 2007.

Recommendation 4. *Review and assess Management progress in implementing closed circuit TV cameras in the Multi Purpose Building (housing the data center).*

Management concurs with this recommendation, which will be implemented in conjunction with other enhancements to the data center.

Appendix. Management Comments