QUALITY CONTROL REVIEW OF CONTROLS OVER THE ENTERPRISE SERVICES CENTER

Department of Transportation

Report Number: QC-2011-001

Date Issued: October 5, 2010

Memorandum

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

Subject: ACTION: Quality Control Review of Controls Over the Enterprise Services Center, Department of Transportation Report No. QC-2011-001

Date: October 5, 2010

From: Earl C. Hedges
Acting 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 our annual review of general, application, and operational controls over the Department of Transportation's (DOT) Enterprise Services Center (ESC). As a Federal service provider, the ESC provides financial management support services to Federal agencies, including accounting, financial management, systems and implementation support services, customer services, and telecommunications and data center services. In addition to DOT, the Center supports the National Endowment for the Arts, the Institute of Museum and Library Services, the Commodity Futures Trading Commission, Consumer Products Safety Commission, National Credit Union Administration, and the Government Accountability Office. It is staffed by Federal Aviation Administration (FAA) employees at the Mike Monroney Aeronautical Center in Oklahoma City, under the direction of DOT's Chief Financial Officer.

The Office of Management and Budget (OMB) requires Federal service providers either to (1) provide their user organizations with independent audit reports on the design and effectiveness of internal controls, or (2) allow user auditors to perform tests of controls at the service organizations.[1] This audit covered both the Delphi Financial Management System[2] and the Consolidated Automation System for Time and Labor Entry (CASTLE) hosted at the ESC. CASTLE is used to support DOT operations only.

[1] OMB Memorandum M-08-24
[2] The Delphi system includes ESC PRISM, a federal acquisition system.

Clifton Gunderson, LLP, of Calverton Maryland, completed this audit under contract to the Office of Inspector General (OIG). OIG staff performed a quality control review of the firm's audit work to ensure that it complied with generally accepted government auditing standards and the American Institute of Certified Public Accountants' Statement on Auditing Standards-70 (SAS-70). SAS-70 requires auditors to determine whether or not service organizations: (1) fairly described their controls; (2) suitably designed the controls; and (3) effectively implemented the controls. Our review disclosed no instances in which Clifton Gunderson did not comply in all material respects with applicable auditing standards.

Clifton Gunderson concluded that ESC described its controls fairly in all material respects, and that the controls were suitably designed to meet stated control objectives. Clifton Gunderson also found that the tested controls operated with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified by management were achieved from October 1, 2009 through June 30, 2010. However, the firm also found that ESC's configuration management controls did not operate effectively and impacted the Center's access controls. Specifically, the Delphi system operated on a database for which the vendor stopped providing security updates in February 2009. Furthermore, ESC did not apply in a timely manner critical security updates that the vendor had provided, and did not assess the system for vulnerabilities and risks associated with the vulnerabilities. Clifton Gunderson's recommendations to correct these and other control deficiencies appear in the Exhibit to this report.

In his September 29, 2010, response to OIG, the Deputy Chief Financial Officer concurred with the recommendations and committed to implementing corrective actions (see the Appendix in this report).

In accordance with DOT Order 8000.1C, the corrective actions taken in response to Clifton Gunderson's recommendations are subject to follow-up. Clifton Gunderson performed additional testing and provided a follow-up management letter to OIG dated September 30, 2010, reporting no significant changes to the control environment between July 1 and September 30, 2010. Clifton Gunderson's follow-up letter did not include any further corrective actions.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (410) 962-1729 or Nathan Custer, Program Director, at (202) 366-5540.

Attachments

#

cc: Chief Information Officer, DOT
Deputy Chief Financial 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, AAE-001

EXHIBIT. RECOMMENDATIONS OF CLIFTON GUNDERSON, LLP, INDEPENDENT AUDITOR

Clifton Gunderson LLP made the following recommendations during its review of general, application, and operational controls over the DOT ESC in fiscal year 2010. OIG agrees that DOT management should implement the following actions to enhance ESC controls.

Configuration Management	
1	Promptly upgrade Delphi's operating system platform to an Oracle certified operating system.
2	Apply software security patch releases on a timely basis.
3	Ensure the system's authorizing official is promptly informed and a risk acceptance is received for any critical or high vulnerabilities that are not addressed. If the risk acceptance lapses, or the situation changes, the authorizing official should renew the acceptance of the risk. Closed in follow-up.
4	Follow Federal and Department guidance in applying critical patch updates on the required timelines.
Access Controls	
5	Implement effective authentication and authorization controls for the audit log server. Closed in follow-up.
6	Implement proper mechanisms to track all contractors who separate from the ESC. Closed in follow-up.
7	Enforce contract clause requiring contractors to communicate in a timely manner all terminated employees. Closed in follow-up.
Security Management	
8	Ensure the CASTLE information system security plan is updated to reflect current operating procedures and any changes made are reviewed in a timely manner. Closed in follow-up.

APPENDIX. MANAGEMENT COMMENTS

September 29, 2010

MEMORANDUM TO: Earl Hedges
Acting Assistant Inspector General
for Financial and Information Technology Audits

FROM: David J. Rivait
Office of the Assistant Secretary for Budget and
Programs/Deputy Chief Financial Officer

SUBJECT: Management Response to the SAS 70 Audit of ESC's
Services Information Security Controls

The Department provides diligent oversight as it works to ensure the quality, accuracy, and integrity of the services provided by the Enterprises Services Center (ESC). The Office of Inspector General's (OIG) annual SAS 70 audit is as administered this year by its contractor, Clifton Gunderson (CG) is integral to these efforts. Once again this year the audit offers considerable insights and fresh perspectives that enable us to further improve our already strong management and controls over financial systems in this ever-changing cyber security environment.

CG issued a qualified opinion on the SAS-70 audit stating that the Delphi database was unsupported; however, upon further detailed review, we have determined that the software remains supported by Oracle and will continue to be until we move the system to an updated version of the software. Subsequent to CG's report, we provided the OIG with detailed documentation including statements by Oracle regarding system support and our analysis. That analysis determined the Delphi environment is fully supported by Oracle and has never been in a non-support status. This conclusion was confirmed through our discussions with, and documentation provided by Oracle. The current Delphi process of mitigating user and system controls will continue to address any vulnerabilities including unauthorized database access, service disruption, data loss or manipulation. As a result, while the Department is planning to upgrade Delphi's operating system, the existing operating system will continue to be supported through the upgrade. We will continue working through this issue with the OIG to convey a full appreciation of the issues, the status of ongoing operations and our plans moving forward.

The Department concurs with CG's other recommendations and has identified corrective actions to remediate the findings. Consistent with past practices, ESC has worked with the auditors throughout this year's SAS 70 audit to identify and schedule corrective actions as audit findings are documented, to ensure swift and appropriate management action. These corrective action plans will be forwarded to you under separate cover prior to October 1, 2010.

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, ESC has demonstrated its strong commitment to ensuring that it's Financial Management Services meet or exceed all information security requirements.

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

cc:
Maria Dowds, Joann Adam, Laurie Park, Wendy Calvin, Marshal Gimpel, Mike Upton, Keith Burlison, Bo Peeler, Steve Aube, Janet Shell, Nina Boyle, Kent Mitchell