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-2010-001

Date: October 1, 2009

From: Rebecca C. Leng Rebecca 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 our annual review of general, application, and operational controls over the Department of Transportation's (DOT) Enterprise Services Center (ESC). ESC is one of four federal service providers designated by the Office of Management and Budget (OMB) to provide financial management systems and services to other Federal agencies. ESC services include accounting, financial management, systems and implementation support, customer services, media solutions, telecommunications, and data center services for DOT and other Federal organizations. In addition to serving DOT, ESC supports the National Endowment for the Arts, the Institute of Museum and Library Services, the Commodity Futures Trading Commission, and the Government Accountability Office. ESC is staffed by Federal Aviation Administration (FAA) employees at the Mike Monroney Aeronautical Center in Oklahoma City, under the direction of the Department's Chief Financial Officer.

OMB requires Federal service providers to either (1) provide its user organizations with an independent audit report on the effectiveness of internal controls or (2) allow user auditors to perform appropriate tests of controls at the service organizations. [1] This audit covered both the Delphi Financial Management System 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.

The audit was completed by Clifton Gunderson, LLP, of Calverton, Maryland, under contract to the Office of Inspector General (OIG). OIG staff performed a quality control review of the audit work to ensure that it complied with applicable standards. These standards include generally accepted government auditing standards and American Institute of Certified Public Accountant's Statement on Auditing Standards–70 (SAS-70). SAS-70 requires auditors to determine whether (1) management fairly presented its description of controls, (2) suitably designed the described controls, and (3) effectively implemented the controls. In our opinion, Clifton Gunderson's audit work complied with these standards.

Clifton Gunderson concluded that management presented its description of ESC controls fairly in all material respects, and that the controls, as described, were suitably designed for all stated control objectives. With regard to implementation, Clifton Gunderson found that the tested controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified by management were achieved from October 1, 2008, through June 30, 2009. However, the report highlighted two exceptions to this finding: ineffective access controls and inadequate segregation of duties. Ineffective access controls allowed CASTLE database administrators (DBA) to share privileged system access and provided no evidence that system activity logs were being reviewed. Inadequate segregation of duties allowed one development DBA to read any table within the production environment as well as to access the production database. Clifton Gunderson made recommendations to correct these control deficiencies.

Clifton Gunderson made additional recommendations to DOT management for improving controls in service continuity, configuration management, security management, and other areas. We agree that implementing these recommendations will further enhance controls over ESC operations and have included these recommendations in the Exhibit.

In a September 30, 2009, response to OIG, the Acting Deputy Chief Financial Officer concurs 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 audit follow-up. Clifton Gunderson performed additional testing and provided a follow-up management letter to OIG on September 30, 2009, reporting no significant changes to the control environment between July 1, 2009, and September 30, 2009. Clifton Gunderson's follow-up letter did not include any further corrective actions.

We appreciate the courtesies and cooperation of FAA, 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) 366-1407 or Nathan Custer, Program Director, at (202) 366-5540.

Attachments

#

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 2009 independent auditor's report on the review of general, application, and operational controls over the DOT ESC. OIG agrees that DOT management should implement the following actions to enhance ESC controls.

Access Controls	
1	Ensure that procedures are developed for regularly reviewing Database Administrator activity by non-Database Administrator personnel. Also, management should document the review of Database Administrator activity.
2	Ensure there is a process in place which requires the security officers to submit Kintana requests requesting reactivation of Delphi user accounts to include duration of reactivation period. Closed in followup.
3	Ensure the Delphi bi-weekly report runs in a consistent manner without interruption. Closed in followup.
4	Ensure the Delphi Information System Security Officer (ISSO) and her team performs quarterly Delphi user access recertifications in a timely manner. Closed in followup.
5	Develop a process that monitors Security Officers' compliance with user recertification and implement measures for non-compliance. Closed in followup.
6	Eliminate the usage of generic user and system level accounts in ESC PRISM, thereby enforcing appropriate user accountability. Closed in followup.
7	Ensure that access authorization forms are completed and documented for all users requiring access to ESC systems.
8	Consider increasing the frequency of server vulnerability scans; require each new, upgraded, or restored system to be scanned for vulnerabilities prior to being placed in production.
Segregation of Duties	
9	Ensure that Database Administrators have named accounts for the proper segregation of duties and user accountability.
Service Continuity	
10	Develop an ESC-wide Continuity of Operations Plan.
11	Develop a tailored plan for the Office of Customer Services (AMO) to meet the standards identified in NIST SP 800-34. The plan should also be updated at least on an annual basis to reflect AMO's current environment.

Configuration Management	
12	Ensure that definitive time frames are in place for the application of Oracle critical patch updates (CPU) or document the testing results that indicate the incompatibility of each CPU.
13	Maintain updated baseline configuration information for all systems and use the updated information to address known vulnerabilities.
Security Management	
14	Ensure that all Memoranda of Understanding are renewed and approved with appropriate authorizing signatures prior to expiration.
15	Implement proper mechanisms to ensure that the separation process is followed appropriately for every separating employee/contractor and that all exit clearance forms are properly filled out and maintained.
16	Ensure that the Delphi Information System Security Plan is updated and formalized with current personnel responsible for security, in accordance with federal guidance. Closed in followup.

APPENDIX. MANAGEMENT COMMENTS

September 30, 2009

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

FROM: Lana Hurdle
Office of the Assistant Secretary for Budget and
Programs/CFO
Acting Deputy Chief Financial Officer

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

Thank you for the Statement on Auditing Standards (SAS) 70 audit of Oklahoma City's Enterprise Services Center's (ESC) Information Security Controls. The Department appreciates the Office of Inspector General's (OIG) coordination and Quality Control Review of Clifton Gunderson's SAS 70 audit, which offers considerable insights that enable us to further improve our already strong management and controls over financial systems in this ever-changing cyber security environment.

The Department concurs with Clifton Gunderson's recommendations and has identified corrective actions to remediate the findings (see attachment). 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.

The Department appreciates the assistance you and your staff have provided throughout the SAS 70 process. The SAS 70 process helps to ensure that ESC continues to strengthen the design and implementation of all controls of our shared service offerings every year, and we look forward to your continued 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, 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.

Attachment: Corrective Action Plan

cc:
Maria Dowds, Joann Adam, Laurie Howard, Wendy Calvin, Terry Burke, Lindy Ritz, Stan Sieg, Marshal Gimpel, Mike Upton, Sara Smith, Keith Burlison, Bo Peeler, Mike Myers, Steve Aube, Robert Stevens, Janet Shell, Nina Boyle, Kent Mitchell

B30:WCalvin:mv:9-30-09
Hdrive/mvicks
MEMOMgmtResponsetoSASAuditofESCServiceWendyC.

Attachment

Corrective Action Plan
For ESC's FY 2009 SAS-70 Audit

NFR #03: Delphi Terminated User Account Deactivation
CG Recommendation 2: There is a process in place, which requires the Security Officers to submit Kintana requests for reactivation of Delphi user accounts to include duration of reactivation period.

Management Response: A revised process was implemented on April 27, 2009, for reactivation of deactivated users. Delphi security officers are required to enter a Kintana request providing justification for user account reactivation. The users will be reactivated for 24 hours only. At the time of reactivation, the end-date is entered so the user account is deactivated in 24 hours. If security officer requests the user account be active for longer than 24 hours, additional justification is required. This action is complete.

CG Recommendation 3: The Delphi bi-weekly report runs in a consistent manner without interruption.

Management Response: The Delphi bi-weekly report program has been automated as of May 5, 2009. This action is complete.

NFR #04: Delphi MoUs
CG Recommendation 14: We recommend ESC management ensures all Memorandum of Understanding (MOU's) are renewed and approved with appropriate authorizing signatures prior to expiration.

Management Response: A new process has been implemented to monitor MOU's for Delphi systems. The ISSO will seek to have an MOU approved and signed by the systems Authorizing Official prior to the expiration of an existing MOU. If the MOU has not been signed within 30 days of expiration it will be elevated to the Authorizing Official to be disconnected or for a risk acceptance. The revised estimation completion date is September 30, 2009. POC: Carol Moffat.

NFR #05: Employee Termination
CG Recommendation 15: ESC Management should implement proper mechanisms to ensure the separation process is followed appropriately for every separating employee/contractor and all exit clearance forms are properly filled out and maintained.

Management Response: In coordination with the Aeronautical Center Director (AMC-1), Human Resource Management (AMH), and Office of Acquisition Services (AMQ), ESC implemented a cross-MMAC initiative to address this issue campus-wide, including all organizations and tenants resident on the MMAC campus. This includes reviewing and updating clearance processes, if needed, to ensure the out-processing forms are properly filled out and maintained for separating MMAC-wide employees/contractors. This action was completed on September 1, 2009. POC: Kent Mitchell.

NFR #07: Delphi User Access

CG Recommendation 4: Ensure the Delphi ISSO and her team performs quarterly Delphi user access recertification's in a timely manner.

Management Response: The Delphi Quarterly Reports became online reports in July, 2009. The Delphi Security Officers (SO) are able to run these reports in real time.

Each quarter the ISSO will send the SO's an e-mail, copying their manager, requiring them to verify they have reviewed all their user accounts. Confirmation is required for all valid accounts. A Kintana request must be submitted for modifying user accounts or deleting invalid user accounts.

Noncompliance from the SO's will cause a second e-mail to be sent directly to their managers. It will then become their manager's responsibility to ensure the SO responds in a timely manner to the ISSO. If the ISSO does not receive a response from the SO within a timely manner, the Operating Administration (OA) Chief Financial Officer (CFO) and the Department of Transportation (DOT) ISSM will be notified by the ISSO.

Specifically, the following actions will be implemented:

1. Implementation of a real time online user account report which SO's can run daily, if desired.

   a. Each quarter the ISSO will send the SO's an email, copying their manager, requiring them to verify they have reviewed all their user accounts. Confirmation is required for all valid accounts. A Kintana must be submitted for modifying user accounts or deleting invalid user accounts.

   b. Noncompliance from the SO's will cause a second e-mail to be sent directly to their managers. It will then become their manager's responsibility to ensure the SO responds in a timely manner to the ISSO.

2. Training for all Delphi SO's prior to the online user account program going into production.

3. Investigate requiring Delphi SO's and their managers to take yearly refresher training as a requirement for their position.

4. Require Rules of Behavior be signed yearly by SO's and their managers listing the requirements of their positions.

Revised estimated completion date is September 30, 2009. POC: Carol Moffat.

CG Recommendation 5: Develop a process that monitors Security Officers compliance with user recertification and implement measures for non-compliance.

Management Response: Management agrees the process can be strengthened but does not agree with the recommendation since the following existing processes are in place.

To further strengthen the process, ESC will ensure that the Delphi incompatibility reports are run and followed up on a timely basis.

Processes have been implemented, due to prior audit findings, to monitor Delphi Security Officers (SO) compliance for user recertification including:

1. Running the Delphi Incompatibility Report

    a. Run weekly for verification of incompatibilities based on the Delphi Roles and Responsibility Matrix

2. Purchasing and implementing "Sox Out of the Box"

    a. COTS package that automatically checks for user compliance

3. Developing and implementing the Delphi Biweekly Auto-Termination program

    a. This program checks for invalid user accounts. It matches employee records against terminated employee files to validate user accounts. In addition, the user accounts that are listed in the report are manually verified by the ISSO. Kintana's are submitted for any user accounts that are not end-dated.

The revised estimated completion date is September 30, 2009. POC: Carol Moffat.

NFR #08: ESC Prism User Accounts

CG Recommendation 6: ESC management should eliminate the usage of generic user and system level accounts in ESC PRISM, thereby enforcing appropriate user accountability.

Management Response: The ESC PRISM generic user accounts, "SYSADMIN" and "SITEADMINGAO", were deactivated when identified by the audit team. ESC has implemented auditing of the ESC PRISM user accounts on a monthly basis. This action was completed by April 20, 2009. POC: Carol Moffat.

NFR #09: COOP

CG Recommendation 10: Develop an ESC-wide Continuity of Operations Plan, as well as a tailored plan for the Office of Customer Services (AMO) to meet the standards identified in NIST SP 800-34. The plan should also be updated at least on an annual basis to reflect AMO's current environment.

Management Response: ESC concurs that a COOP is needed for ESC, including two of ESC's directorate level organizations (AMO, and AMZ). ESC's AMI organization will lead the completion of these COOP's. The project, which started in April 2009, is expected to last approximately six (6) months. This will be completed by October 31, 2009. POC: Charles Hall.

NFR #10: DBA Accounts

CG Recommendation 9: ESC management ensure that CASTLE, Delphi and ESC Prism DBA have named accounts for the proper segregation of duties and user accountability.

Management Response: A single Oracle system level account (not a named user account) was shared on CASTLE. The user's privileges that had access to this account were revoked on August 5. Named accounts will be created for DBAs that support ESC PRISM, CASTLE, and Delphi. Rules of behavior for DBA's will be updated to reflect that only named accounts will be used except in special circumstances. The estimated completion date is October 31, 2009. POC: Christopher Carl.

CG Recommendation 1: ESC management should ensure that procedures for regularly reviewing DBA activity by non DBA personnel. Also, management should document the review of DBA activity.

Management Response: The Work Instructions for systems monitoring will be updated. This will allow read access and restricted mode session access to be revoked. The estimated completion date is October 31, 2009. POC: Christopher Carl, AMI-310.

We concur with the condition that proof of audit review for CASTLE and ESC PRISM was not provided and that reviews were not conducted by non-DBA personnel regularly.

The procedures will be updated where needed and automated tools will be implemented, so that non-DBA personnel review DBA activity with subsequent reviews by management. The estimated completion date has moved up to December 31, 2009. POC: Christopher Carl.

CG Recommendation 12: ESC management should ensure that definitive timeframes are in place for the application of ORACLE CPUs or document the testing results that indicated incompatibility of each CPU.

Management Response: The Delphi Oracle patches (July 2008) referenced from within the Risk Acceptance was applied in February 2009. Patches from October 08 and January 09 had been reviewed and documented according to the CPU Patch work instruction, AMEWI-0001. This documentation was provided within the PBC requests.

The CPU patch work instruction, AMEWI-0001, is in the process of being updated to include a formal CPU patch review document to assist us with prioritizing the CPU patches into our release schedule. This documentation will be complete by October 31, 2009. POC: Michelle Overstreet, AME-210.

Data from the NGSSquirrel scan will be analyzed to determine if enhanced named and system account auditing can be enabled. If any additional system account audits are identified, they will be enabled after being tested. The estimated completion date has moved up to December 31, 2009. POC: Christopher Carl.

NFR #12: Telecommunications LAN & Voice

CG Recommendation 8: Management should consider increasing the frequency of server vulnerability scans; require each new, upgraded, or restored system to be scanned for vulnerabilities prior to being placed in production.

Management Response: ESC is currently scanning its servers multiple times a month with FoundStone, the DOT/FAA enterprise vulnerability scanning tool. A quarterly Nessus scan is also performed on the servers supporting Delphi, CASTLE and ESC PRISM.

ESC will create a policy memo for ESC supported systems to follow. The memo shall require system administrators to request vulnerability scan for new servers, or any existing server undergoing major upgrades or being restored before the server can be placed back into production. This action was completed July 31, 2009. POC: Huey Grantham, AMI-510.

CG Recommendation 13: Management should maintain updated baseline configuration information for all systems and use the updated information to address known vulnerabilities.

Management Response: ESC is working on a process for baseline configuration information. The ESC System Management Facility (SMF) is implementing the CiRBA (Configuration item Request Broker Architecture) baseline configuration for servers managed by the ESC SMF. The estimated completion date for the CiRBA baseline configuration implementation is December 31, 2009. POC: Huey Grantham, AMI-510.

NFR #13: ESS/Delphi

CG Recommendation 16: The Delphi Information System Security Plan be updated and formalized with current personnel responsible for security in accordance with federal guidance.

Management Response: The Delphi Information System Security Plan (ISSP) has been updated to identify current personnel responsible for security for Delphi. The estimated completion date is October 16, 2009. POC: Carol Moffat, AMI-510.

CG Recommendation 7: ESC management ensures access authorization forms are completed and documented for all users requiring access to ESC systems.

Management Response: ESC Management agrees that access authorization forms must be completed and documented. The Kintana access authorization process is in place with requests documented and available for audit. The process has been managed by the Delphi Application Administrators since January 2009, to ensure access request forms are completed and maintained. The estimated completion date is October 16, 2009. POC: Carol Moffat, AMI-510.