QUALITY CONTROL REVIEW OF THE REPORT ON CONTROLS OVER THE ENTERPRISE SERVICES CENTER

Department of Transportation

Report Number: QC-2008-079
Date Issued: September 22, 2008

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 Services Center
Report No. QC-2008-079

Date: September 22, 2008

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 the review of general, application, and operational controls over the Department of Transportation's (DOT) Enterprise Services Center (ESC). The ESC performs services including accounting; financial management; systems and implementation; media solutions; telecommunications; and data center services for DOT and other Federal organizations. It 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 (CFO).

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 governmental agencies. 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. OMB requires Federal Service Providers to obtain an independent audit in accordance with the American Institute of Certified Public Accountants' (AICPA) Statement on Auditing Standards.

This year's audit of the DOT ESC was expanded to cover not only the Delphi Financial Management System but also the Consolidated Automation System for Time and Labor Entry (CASTLE). CASTLE is used to support DOT operations only. The audit was completed by Clifton Gunderson, LLP, of Calverton, Maryland, under contract to the Office of Inspector General (OIG). We 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 AICPA's 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 ESC presents fairly, in all material respects, the controls that had been placed in operation as of June 30, 2008. In addition, the independent auditor concluded that controls, as described, are suitably designed for all stated control objectives except in the areas of logical access and segregation of duties concerning CASTLE system operations.[1] Specifically, the CASTLE Database Administrators had access to develop, test, and release system changes into production without any independent review and approval.

Gunderson also reported that the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified by management were achieved during the period from October 1, 2007, through June 30, 2008.

Gunderson made 19 recommendations to DOT management for improving controls in various areas, including access, accounting operations, service continuity, segregation of duties, security planning, and management. We agree that implementing these recommendations will further enhance controls over operations of the ESC and have included these recommendations in the Exhibit to this report. In a September 17, 2008, response to OIG, the Acting 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 prepare a follow-up management letter to OIG by September 30, 2008, reporting whether the control environment changed significantly between July 1, 2008, and September 30, 2008. After receiving Gunderson's follow-up letter, we will decide whether additional information is needed for any planned corrective actions, including target completion dates.

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

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 2008 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	Management should ensure that proper mechanisms are in place ensuring timely and proper revocation of all access for terminated employees.
2	Management should perform testing of database updates and either apply the patches or document the issues with the patches that prevent operational deployment. In the event that an update cannot be deployed, management should document compensating controls to reduce the likelihood of an individual vulnerability being exploited.
3	Management should audit powerful system and database administrator accounts on the database platforms for certain commands. This will provide management with an audit trail of actions taken by powerful authorized accounts.
4	Management should periodically perform wireless scans for rogue access points and remove all unauthorized devices from the Mike Monroney Aeronautical Center internal network.
5	Management should continue with its migration plans for the Delphi systems.
6	Management should set the failed login attempts setting as required by DOT policy, and set the password lock setting to unlimited to suspend the account, requiring the Helpdesk to unlock or reset the password to the account.
7	Management should ensure that no Delphi acquisitions and procurement software client uses generic user accounts, in order to enforce proper user accountability.
Accounting Operations	
8	Management should ensure all agencies adhere to standard procedures for project/agreement close-out.

Service Continuity	
9	Management should review and revise its Continuity of Operations Plan to meet the standards identified in NIST SP 800-34. The plan should also be updated at least on an annual basis to reflect the ESC's current environment.
10	Management should develop and formalize maintenance agreements between its Media Solutions Division and all of its vendors to ensure that operations downtime is minimized.
11	Management should ensure the Enterprise Support Systems system Disaster Recovery plan is finalized and approved.
Segregation of Duties	
12	Management should ensure that programmers' and database administrators' access to production and development is segregated, and ensure that changes are tested in development and released into production by different individuals.
Security Planning	
13	Management should, in collaboration with the various contracting officer technical representatives, perform a review of all contractors who have separated and ensure that their access to system resources has been revoked and their key cards/badges deactivated. Management should ensure that proper measures are taken to ensure that the separation process is followed closely for every separating employee/contractor and that all exit out-processing forms are properly filled out and maintained.
14	Management should ensure that signed Rules of Behavior (RoB) forms are obtained for every system user (if not already on file) and improve procedures to ensure that RoB forms are signed prior to granting users system access. Alternatively, management should implement automated RoB on each ESC information system so that the user has to read, acknowledge, and agree to follow the rules of behavior before access to an information system is authorized.
15	Management, through the Information Systems Security Division, should perform monthly password cracking/auditing checks to ensure that ESC systems have password filters permanently set to enforce password complexity (alphanumeric and special characters).
16	Management should ensure that the Certification Agent/s in the security certification and accreditation process of the System Management Facility 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.

17	Management should ensure memorandums of understanding (MOU) are updated prior to expiration and contain the authorizing signatures for implementation.
	Management
18	ESC management should ensure that the management assertions accurately reflect the current environment and that said controls are implemented and operating as designed.
19	ESC management should ensure that the responsibility for the reconciliation of outbound data is clearly delineated within the memorandum of understanding (MOU) with ESC clients.

APPENDIX. MANAGEMENT COMMENTS

September 17, 2008

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

FROM: Lana Hurdle
Acting Deputy Chief Financial Officer

SUBJECT: Management Response to the Statement on Auditing Standards (SAS) 70 Audit of the Enterprise Services Center (ESC's) Services Information Security Controls

Thank you for the SAS 70 audit of Oklahoma City's ESC's Information Security Controls. We appreciate the Office of Inspector General's (OIG) coordination and Quality Control Review of Clifton Gunderson's SAS-70 audit.

We concur with Clifton Gunderson's recommendations and have identified corrective actions to address them (see attachment). Consistent with past practices, we have worked with the auditors throughout this year's SAS-70 audit to ensure that as issues are documented corrective actions are also identified and scheduled to mitigate risks and to strengthen ESC's controls. Corrective actions already taken to enhance ESC's security in response to this year's SAS-70 audit include:

Access Controls:

- Implemented a procedure which ensures that all Delphi User-IDs assigned to terminated personnel are turned off at the appropriate end-date.
- Established and performed processes for monthly and quarterly wireless scans.
- Continued migration activities for Delphi isolation. Host-based firewalls have been implemented on test systems.
- Set Failed Login Attempts and Password Lock settings according to Department of Transportation (DOT) policy.
- Disabled Generic User IDs (created unique IDs as needed).

Accounting Operations:

- Requested the Office of Budget-Reimbursable Oversight Division, ABU-500, to include a standard close-out form in their Federal Aviation Administration (FAA) Financial Manual. When FAA projects are closed, the Office of Operational Services (AMZ) will utilize the standard form.

Segregation of Duties:

- Transferred the Consolidated Automated System for Time and Labor Entry (CASTLE) production responsibilities to the Office of Information Technology (AMI) personnel thereby ensuring segregation of duties from CASTLE development personnel in the Office of Application Services (AME).

Security Planning:

- Obtained Risk Acceptance to allow a single person to perform as the Information System Security Certifier (ISSC) and the System Owner (SO) for the Systems Management Facility (SMF). Updated Management Assertions accordingly.
- Revised Memorandum of Understanding (MOU) Procedure which now requires AME to request customer approval of MOUs (3 customer approvals obtained to date).

Management:

- Updated Management Assertions to reflect ESC's current environment (e.g., system operations, organization structure, process workflows, and physical environment).
- Updated the AME MOU template to clearly delineate reconciliation of outbound data responsibility.

The following additional corrective actions are currently underway:

Access Controls:

- Developing process to document management approval and compensating controls, if current ORACLE Critical Patch Updates are not implemented in the next available release schedule.
- Performing feasibility studies for automated audits of system commands.

Service Continuity:

- Developing the AMI and Media Solutions Division Continuity of Operations Plans (COOP).
- Coordinating new equipment maintenance contracts after manufacturer's warranty expires.
- Updating the Enterprise Support Systems Disaster Recovery Plan.

Security Planning:

- Consolidating contractor exit procedures to ensure separated contractor access to ESC-managed resources are terminated.
- Documenting Rules of Behavior (RoB) implementations (automated or paper) and obtaining/storing paper copies per Official Files List (OFL) requirements.

We appreciate the assistance you and your staff have provided throughout the SAS-70 process. We are pleased that we continue to strengthen the design and implementation of all controls for ESC’s 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, we are fully committed to ensuring that ESC’s Financial Management Services meet or exceed all information security requirements.

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

Attachment

Attachment

Corrective Action Plan
For ESC's FY 2008 SAS-70 Audit

NFR #01:

Recommendation 1: In collaboration with the various Contracting Officer's Technical Representative (COTRs), perform a review of all contractors who have separated and ensure their access to system resources has been revoked and their key cards/badges deactivated. Make sure proper measures are taken to ensure the separation process is followed closely for every separating employee/contractor and all exit out-processing forms are properly filled out and maintained.

> An updated clearance procedure will be implemented for ESC-managed systems that mandate out-processing forms for every separating employee/contractor are properly filled out and maintained. The procedure will include notification to the Systems Administrators so that the terminated personnel's access can be revoked. Information Systems Security Officer (ISSOs) will coordinate with the COTRs to perform a review of all contractors separated from January 1, 2008, through date of procedure implementation. Remediation by December 31, 2008.

Recommendation 2: Ensure signed Rules of Behavior forms are obtained for every system user (if not already on file) and improve procedures to ensure RoB are signed prior to granting users system access. Alternatively, implement automated RoB on each Enterprise Services Center (ESC) information system so that the user has to read, acknowledge, and agree to follow the rules of behavior, before authorizing access to an information system.

> Rules of Behavior: The ESC will ensure either signed hard-copy or automated RoBs are obtained from every system user prior to granting users system access to ESC-managed systems. Automated RoBs will be implemented, where appropriate. For system users controlled by hard copy RoBs, updated signed RoBs will be obtained at frequencies specified within each system's respective Security Plan. Remediation by December 31, 2008.

NFR #03:

Recommendation 1: Review and revise their Continuity of Operations Plan to meet the standards identified in the National Institute of Standards and Technologies (NIST) SP 800-34. The plan should also be updated at least on an annual basis to reflect the ESC's current environment.

Management concurs with these recommendations. The Management Systems Division (MSD) will develop a COOP specific to the media solutions work environment using the components recommended by the NIST 800-34 Federal Guidelines. Development of the MSD COOP and subsequent annual review/update will be completed by October 2008 and October 2009, respectively through the Media Solutions Division, AMI-700, quality assurance specialist coordination efforts. Remediation by October 15, 2008.

Recommendation 2: Develop and formalize maintenance agreements between Media Solutions Division and all of its vendors to ensure operations downtime is minimized.

> Management concurs with this recommendation. The MSD management will coordinate the establishment of a new AVID equipment maintenance contract before expiration of the year-long manufacturer warranty on the new AVIDs. Remediation by March 1, 2009.

NFR #04:

Recommendation 1: We recommend that ESC management ensures the Certification Agent(s) in the Security Certification and Accreditation process of the SMF general support system be an individual, group, or organization that retain/s an appropriate level of independence and remains free from conflicts of interest.

> Management concurs with this recommendation. A risk acceptance is documented and was signed by the Authorizing Official (AO) on February 22, 2008, for the ISSC and SO being the same person for the SMF. The Information System Security Division, AMI-500, will update the management assertions to reflect the independence of AMI-500 in relation to the auditing of systems within DOT, FAA, and other government agencies. Remediation by October 31, 2008.

NFR #05:

Recommendation 1: We recommend ESC management should ensure proper mechanisms are in place to ensure timely and proper revocation of all access for terminated employees.

> Management concurs with this recommendation. ESC Management agrees that proper mechanisms must be in place to ensure terminated employee’s access to the Delphi system is deactivated in a timely manner. If a terminated employee has multiple user accounts, the Automatic User Termination Program is currently only deactivating the first user account it finds, but is not deactivating any subsequent accounts that individual might have. To correct this, Kintana #244118 was submitted on June 6, 2008, requesting the program be modified to ensure all user accounts assigned to an employee are appropriately deactivated by the Automatic User Termination program. This System Change Request (SCR) is currently scheduled to be implemented in the December 7, 2008 Delphi release. In the interim, the ISSO staff has created the Automatic User Termination Verification Procedure in the ISSO Desk Guide. This procedure was implemented on

> June 16, 2008, and it is to be run by the ISSO staff for all individuals identified on the Automatic User Termination Report, each time the program runs. The addition of this procedure ensures that any and all Delphi User-IDs assigned to those individuals identified on the Automatic User Termination Report have been appropriate end-dated. The ISSO staff has begun attaching their verification to the Automatic User Termination Report, per the new Automatic User Termination Verification Procedure guidelines. Remediation by December 31, 2008.

NFR #06:

Recommendation 1: Management should perform testing of Oracle Critical Patch Updates (CPUs) and either apply the patches or document the issues with the patches that prevents operational deployment. In the event that a CPU cannot be deployed, management should document compensating controls to reduce the likelihood of an individual vulnerability being exploited.

> AME management agrees with the recommendation to perform testing of Oracle CPUs and either apply the patches or document the issues with the patches that prevent operational deployment. ESC will implement a process to obtain appropriate documentation, including management approval, supporting the reason for any delays in the deployment of CPUs, in the event implementation of current CPU patches cannot be integrated into the next release schedule. Remediation by December 31, 2008.

Recommendation 2: Management should audit powerful system and database administrator accounts on the Oracle database platforms for the CREATE, ALTER, and DROP commands. This will provide management with an audit trail of actions taken by powerful authorized accounts.

> AME will perform extensive testing and evaluation to examine potential operational impacts on the performance of the database servers. We are further researching the implications. Remediation by March 31, 2009.

Recommendation 3: Management should centrally maintain documentation of risk acceptances and false positives resulting from vulnerability and penetration testing.

> Since this SAS-70 crossed different systems that have different Information Systems Security Officer (ISSOs), the AOs, and system owners, centralizing the false positives and risk acceptances will require a database to track. AMI-500 will pursue the development of a database to track the risk acceptance and false positive repository for ESC. Remediation by December 31, 2008.

Recommendation 5: Periodically perform wireless scans for rogue access points and remove all unauthorized devices from the Mike Monroney Aeronautical Center (MMAC) internal Network.

AMI-500 will perform periodic testing on both a monthly and quarterly basis using different tools to search for rogue devices. The monthly scans will utilize the AMC ARC Foundstone wireless assessment discovery module (currently being tested) and the quarterly scans will consist of the NETStumbler wireless scanning tool. Remediation by October 1, 2008.

Recommendation 6: Management should continue with its migration plans for the Delphi systems.

The Delphi Authorizing Official has accepted any perceived risks associated with the Delphi security enclave (Delphi Enclave approval memo signed June 12, 2008). Implementation of the security enclave is associated with the Delphi Hardware upgrade. In addition to current mitigation strategies, host-based firewalls will be implemented by March 31, 2009,to provide additional security. (Note that Delphi systems are scheduled to be moved to their own IP space by September 30, 2009). Remediation by March 31, 2009.

NFR #07:

Recommendation 1: Ensure all agencies adhere to standard procedures for project / agreement close-out.

The General Accounting Division, AMZ-300, will work with Office of Budget-Reimbursable Oversight Division, ABU-500, to have a standard close out form included in the Reimbursable Agreements Chapter of the FAA Financial Manual and the rest of the department will follow work instruction AMZWI-30002 which requires an official close-out memo for each reimbursable agreement. Remediation by October 01, 2008.

NFR #08:

Recommendation 1: We recommend that ESC ensures Management Assertions accurately reflect the current environment and that said controls are implemented and operating as designed.

The Printing and Graphic Team, AMI-900, will update its Management Assertions to reflect the current operating environment. The AMI-900 will also develop an Organizational Chart, augmented by an Excel spreadsheet that contains all theAMI-900 employees with their Roles and Responsibilities identified. We will utilize and provide a system generated list of the AMI-900 Federal employees. Remediation by October 30, 2008.

The Office of Information Technology (AME) Management agrees that the AME section of the Management Assertions will be updated to accurately reflect the current AME environment prior to the next SAS-70 audit. Remediation by October 30, 2008.

Recommendation 2: We recommend that ESC ensures the ESS DR plan is finalized and approved.

> The ESS DR test plan will be sent to the Authorizing Official for final approval once final updates have been applied. Remediation by October 30, 2008.

Recommendation 3: We recommend that ESC ensures the responsibility for the reconciliation of outbound data is clearly delineated within the Memorandum of Understanding (MOU) with ESC clients.

> The AME MOU template will be updated to clearly delineate the responsibility for the reconciliation of outbound data. Remediation is complete.

NFR #09:

Recommendation 1a: Set the Failed Login Attempts setting to 3 invalid attempts to adhere to DOT policy.

> The Failed Login Attempts setting will be set to 3 invalid attempts, to adhere to DOT Policy. Remediation by September 30, 2008.

Recommendation 1b: Set the Password Lock setting to unlimited to suspend the account, requiring the Helpdesk to unlock or reset the password to the account.

> The Password Lock setting will be set to unlimited to suspend the account, requiring the Helpdesk to unlock or reset the password to the account. Remediation by September 30, 2008.

Recommendation 2a: Programmers' and DBAs' access to production and development should be segregated.

Recommendation 2b: Ensure changes should be tested in development and released into production by different individuals.

> The CASTLE lead will work with AME management to ensure resources are available to allow for appropriate segregation of duties between CASTLE Programmers and DBAs, to ensure the CASTLE Production Control process for DBA Production Support is consistently followed. Remediation by September 30, 2008.

NFR #10:

Recommendation 1: Ensure MOUs are updated prior to expiration and contain the authorizing signatures for implementation.

> Management concurs with this recommendation. The ESC MOU creation/update procedure will be revamped to ensure MOUs are updated prior to expiration and contain appropriate authorizing signatures for implementation.

NOTE: Updated MOUs with final signatures have now been obtained on the following MOUs: GovTrip, Federal Personnel Payroll System (FPPS), General Services Administration (GSA) NEAR, and OIG and the Transportation Inspection General Reporting System (TIGR). Renewal activities are currently underway for the remaining 9 expired MOUs. Thirteen other MOUs have been renewed (with final signatures) within the past 12 months. Remediation by January 31, 2009.

NFR #11:

Recommendation 1: ESC management should ensure no ESC Prism client uses generic user accounts. This would enforce proper user accountability.

Management concurs with this recommendation. The ESC Prism generic account will be retired, and will be replaced with unique accounts that will enforce proper user accountability. Remediation is complete.