Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Transportation Security Administration Component of the FY 2010 DHS Financial Statement Audit

OIG-11-73

April 2011

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

APR 13 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the FY 2010 Transportation Security Administration (TSA) component of the DHS financial statement audit as of September 30, 2010. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors' Report* dated November 12, 2010 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at the TSA component in support of the DHS FY 2010 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated February 16, 2011, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusions on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

February 16, 2011

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and Chief Financial Officer
Transportation Security Administration

Ladies and Gentlemen:

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS or Department), as of September 30, 2010, and the related statement of custodial activity for the year then ended (herein after referred to as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2010, and the statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources as of September 30, 2010 (hereinafter referred to as "other fiscal year (FY) 2010 financial statements"), or to examine internal control over financial reporting over the other FY 2010 financial statements.

Because of matters discussed in our *Independent Auditors' Report,* dated November 12, 2010, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended. Additional deficiencies in internal control over financial reporting, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended; and had we been engaged to audit the other FY 2010 financial statements, and to examine internal control over financial reporting over the other FY 2010 financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

The Transportation Security Administration (TSA) is a component of DHS. During our audit engagement, we noted certain matters in the areas of information technology (IT) configuration management, access controls, and security management with respect to TSA's financial systems information technology (IT) general controls, which we believe are control deficiencies. These matters are described in the *IT General Control and Financial System Functionality Findings and Recommendations by Audit Area* section of this letter.

Information Technology Management Letter for the TSA Component of the FY 2010 DHS Financial Statement Audit

KPMG LLP is a Delaware limited liability partnership, the U.S. member firm of KPMG International Cooperative ("KPMG International"), a Swiss entity.

The control deficiencies described above are presented in our *Independent Auditors' Report*, dated November 12, 2010. This letter represents the separate limited distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through a Notice of Finding and Recommendation (NFR).

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. We aim to use our knowledge of TSA gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies. We have not considered internal control since the date of our *Independent Auditors' Report.*

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key TSA financial systems and IT infrastructure within the scope of our engagement to audit the FY 2010 DHS financial statements in Appendix A; a description of each internal control finding in Appendix B; the current status of the prior year NFRs in Appendix C; and TSA management's written response in Appendix D. Our comments related to certain additional matters have been presented in a separate letter to the Office of Inspector General and the TSA Chief Financial Officer.

TSA's written response to our comments and recommendations has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of DHS and TSA management, DHS Office of Inspector General, OMB, U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit of DHS' balance sheet as of September 30, 2010 and the related statement of custodial activity for the year then ended, we performed an evaluation of information technology general controls (ITGC) at TSA, to assist in planning and performing our audit. The U.S. Coast Guard's (Coast Guard) Finance Center (FINCEN) hosts key financial applications for TSA. As such, our audit procedures over IT general controls for TSA included testing of the Coast Guard's FINCEN policies, procedures, and practices, as well as TSA policies, procedures and practices at TSA Headquarters. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is further described in Appendix A.

The FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the general IT controls environment.

- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Security management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from contr*olling key aspects of comp*uter-related operations, thus deterring unauthorized actions or access to assets or records.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit, we also performed technical security testing for key network and system devices. The technical security testing was performed both over the Internet and from within select Coast Guard facilities, and focused on test, development, and production devices that directly support TSA's financial processing and key general support systems.

Application controls were not tested for the year ending September 30, 2010 due to the nature of prior-year audit findings.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2010, TSA took corrective action to address prior year IT control deficiencies. For example, TSA made improvements in its own policies and procedures over its own configuration management monitoring controls related to the development, implementation, and tracking of scripts at Coast Guard's FINCEN. However, during FY 2010, we continued to identify IT general control deficiencies that impact TSA's financial data. The key issue from a financial statement audit perspective related to controls over the development, implementation, and tracking of scripts at Coast Guard's FINCEN. Collectively, these deficiencies negatively impacted the internal controls over TSA's financial reporting and its operation. In addition, based upon the results of our test work, we noted that TSA did not fully comply with the Department's requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the four findings issued during our TSA FY 2010 testing, three were repeated findings and one was a new IT finding. These findings represent deficiencies in three of the five FISCAM key control areas. Specifically the deficiencies were: 1) unverified access controls through the lack of comprehensive user access privilege re-certifications, 2) security management issues involving the terminated employee process, and 3) physical security and security awareness issues.

In addition, we determined that the following deficiencies identified at the Coast Guard IT environment also impact TSA financial data: 1) inadequately designed and operating IT script change control policies and procedures, 2) security management issues involving civilian and contractor background investigations, 3) lack of consistent contractor, civilian, and military system account termination notification process, 4) physical security and security awareness issues, and 5) procedures for role-based training for individuals with elevated responsibilities not fully implemented. We also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems that house TSA financial data are not compliant with FFMIA and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control deficiencies, and strengthening the control environment at FINCEN.

These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and TSA financial data could be exploited thereby compromising the integrity of financial data used by management and reported in TSA's financial statements.

While the recommendations made by us should be considered by TSA, it is the ultimate responsibility of TSA management to determine the most appropriate method(s) for addressing the deficiencies identified based on their system capabilities and available resources.

IT GENERAL CONTROLS AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS AND RECOMMENDATIONS BY AUDIT AREA

Findings:

During the FY 2010 DHS Financial Statement Audit, we identified the following TSA IT and financial system control deficiencies that in the aggregate are considered management letter comments. Our findings are divided into two groupings: 1) financial systems controls and 2) IT system functionality.

Related to IT Financial Systems Controls:

Configuration Management

The Coast Guard's core financial system configuration management process controls are not operating effectively, and continue to present risks to TSA financial data confidentiality, integrity, and availability. Financial data in the general ledger may be compromised by automated and manual changes that are not adequately controlled. For example, the Coast Guard uses an IT scripting process to make updates, as necessary, to its core general ledger software to process financial data. We noted that some previously noted weaknesses were remediated (particularly in the second half of FY 2010), while other control deficiencies continued to exist. The remaining control deficiencies vary in significance; however three key areas that impact the Coast Guard IT Script control environment are: 1) Script Testing Requirements, 2) Script Testing Environment, and 3) Script Audit Logging Process.

1) Script Testing Requirements: Limited testing requirements exist to guide FINCEN staff in the development of test plans and guidance over the functional testing that should be performed.
2) Script Testing Environment: Not all script changes were tested in the appropriate test environments.
3) Script Audit Logging Process: FINCEN's core system databases are logging changes to tables as well as successful and unsuccessful logins. However, no reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities and ensure that all scripts run have been approved.

In addition, we noted weaknesses in the script change management process at the USCG as it relates to the Internal Control over Financial Reporting (ICOFR) process (e.g., the financial statement impact of the changes to FINCEN core accounting system through the script change management process).

Access Control

- Access review procedures for key financial applications do not include the review of all user accounts to ensure that all terminated individuals no longer have active accounts; inactive accounts are locked; and privileges associated with each individual are still authorized and necessary.

Security Management

- The computer access agreement and exit clearance procedures for TSA employees have not been consistently implemented; and

- During our after-hours physical security and social engineering testing we identified exceptions in the protection of sensitive user account information. The tables below detail the exceptions identified at the locations tested.

After-Hours Physical Security Testing:

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a TSA employee's / contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at TSA Headquarters.

Exceptions Noted	**Total Exceptions at TSA HQ by Type**
Passwords	0
For Official Use Only (FOUO)	0
Keys/Badges	0
Personally Identifiable Information (PII)	0
Server Names/IP Addresses	0
Unsecured Laptop	1
External Drives	0
Credit Cards	0
Classified Documents	0
Other –US government official passport	0
Total Exceptions at TSA HQ	**1**

Social Engineering Testing:

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or gaining computer system access.

Total Called	**Total Answered**	**Number of people who provided a password**
45	10	3 People Provided Their Passwords

Related to Financial System Functionality:

We noted that financial system functionality limitations are contributing to control deficiencies reported herein, and inhibiting progress on corrective actions impacting TSA. These functionality limitations are preventing the TSA from improving the efficiency and reliability of its financial reporting processes. Some of the financial system limitations lead to extensive manual and redundant procedures to process transactions, verify accuracy of data, and to prepare financial statements. Systemic conditions related to financial system functionality include:

- As noted above, Coast Guard's core financial system configuration management process is not operating effectively due to inadequate controls over the IT script process. The IT script process was instituted as a solution primarily to compensate for system functionality and data quality issues;
- Production versions of operational financial systems are outdated, no longer supported by the vendor, and do not provide the necessary core functional capabilities (e.g., general ledger capabilities); and
- Issues with current technology are preventing TSA management from reviewing account recertification reports timely.

Recommendations:

We recommend that TSA:

- Conduct an assessment over the ICFOR process related to identifying and evaluating scripts that have a financial statement impact, in coordination with USCG. This assessment can be included in the testing of the TSA Script Configuration Management Oversight Process as part of TSA's annual OMB Circular A-123 efforts. Further, we recommend that this assessment (1) be performed early in FY 2011, in time to remediate deficiencies before the end of the third quarter, and (2) involve process documentation and sufficient testing to fully assess both design and operating effectiveness of controls.
- Have FINCEN update its helpdesk procedures to provide the correct guidelines so that its helpdesk staff will no longer grant additional Standard Financial Procurement Desktop roles that were not requested via the Automated Access Request (AAR) process. TSA should closely monitor the requests implemented by FINCEN to ensure that the updated procedures are being followed.
- Improve the timeline and process of its quarterly review. TSA should update its procedures to monitor the timeliness, accuracy and quality of the quality review process.
  - Update quarterly review Internal Standard Operating Procedure to add the expected timeline to complete the quarterly review.
  - Conduct timely follow-up and review of the actual FINCEN implementation of the AARs to ensure that the AARs were implemented as requested.
- Work with FINCEN to identify and implement the best solution to remove the one Sunflower role from the user's profile.
- Work with FINCEN to research and identify options to enhance the automated AAR process.
- Provide more training and oversight for any new access manager to ensure the process is thoroughly followed.
- Closely monitor and follow-up with FINCEN to ensure requests are implemented timely and correctly.
- Review and identify alternate reporting processes in cases of technical difficulties where supervisors cannot access the master files on SharePoint.

- Supervisors and Contracting Officer's Technical Representatives within each program office in TSA should ensure that each TSA employee and contractor have on file a signed Computer Access Agreement form, prior to any financial system access being granted.

- Continue to execute the IT Security Awareness Training program.

- Conduct an internal Physical Security walkthrough on a bi-annual basis.

- Conduct one-on-one training with individuals failing physical security after-hours testing.

- Conduct a communications campaign to address the effects of improper handling of Physical Security.

- Conduct internal Social Engineering testing on a quarterly basis.

- Conduct one-on-one training with individuals failing social engineering attempts.

- Conduct a communications campaign via broadcast warning against social engineering.

APPLICATION CONTROLS

Application controls were not tested for the year ending September 30, 2010, due to the nature of the prior-year audit findings.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from TSA's Chief Financial Officer and Chief Information Officer. Generally, TSA management agreed with our findings and recommendations. TSA management has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments in Appendix D.

OIG Response

We agree with the steps that TSA management is taking to satisfy these recommendations.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2010

Appendix A

Description of Key TSA Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit Engagement

Below is a description of significant TSA financial management systems and supporting IT infrastructure included in the scope of the engagement to perform the financial statement audit.

Locations of Audit: TSA Headquarters in Washington, D.C. and the Coast Guard FINCEN in Chesapeake, Virginia. TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Audit:

- *Core Accounting System (CAS)*: Core accounting system that is the principal general ledger for recording financial transactions for TSA. CAS is hosted at FINCEN, the Coast Guard's primary data center. It is a customized version of Oracle Financials.
- *Financial Procurement Desktop (FPD)*: Used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is hosted at FINCEN.
- *Sunflower:* Sunflower is a customized third party commercial off the shelf product hosted at FINCEN and used for TSA and Federal Air Marshals property management. Sunflower interacts directly with the financial accounting (FA) module in CAS. Additionally, Sunflower is interconnected to the FPD system.
- *MarkView:* MarkView is an imaging and workflow software used to manage invoices in CAS. Each invoice is stored electronically and associated to a business transaction so that users are able to see the image of the invoice. MarkView is interconnected with the CAS system and is located at the FINCEN in Chesapeake, VA and is managed by the United States Coast Guard.

Appendix B

FY 2010 Notice of IT Findings and Recommendations at the TSA

Notice of Findings and Recommendations – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditors' Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist TSA in the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2010

Notification of Findings and Recommendations – Detail

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
TSA-IT-10-01	To complement our IT audit testing efforts as part of the FY2010 DHS Integrated Audit, we also performed social engineering and after hours physical security testing During our testing we identified the following During our after-hours physical security testing, we identified one instance of an unsecured laptop computer; During our social engineering testing, we were provided with three user's passwords.	We recommend TSA in the area of physical Security to: 1) Continue to execute the IT Security Awareness Training program; 2) Conduct an internal Physical Security walkthrough on a bi-annual basis; 3) Conduct one-on-one training with individuals failing physical security after-hours testing; 4) Take administrative actions, if needed, on a case-by-case basis; and 5) Conduct a communications campaign to address the effects of improper handling of Physical Security. We recommend TSA in the area of social engineering to: 1) Continue to execute the IT Security Awareness Training program; 2) Conduct internal Social Engineering testing on a quarterly basis; 3) Conduct one-on-one training with individuals failing social engineering attempts.		X	1

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		4) Conduct a communications campaign via broadcast warning against social engineering.			
TSA-IT-10-02	*Core Accounting System (CAS) & Financial Procurement Desktop (FPD)* During our FY 2010 IT test work, we determined that TSA had created an Internal Standard Operating Procedure (ISOP) to detail how quarterly access reviews were to be performed. We compared a listing of TSA, CAS, and FPD users to the master listing of users who needed modifications or deletions for three quarters (Q1, Q2, and Q3). We did not identify any exceptions for Q1 and Q2; however, for the 3rd quarter, one CAS user was not deleted or modified within 50 days after the end of the completion of the 3rd quarter. In addition, we noted 115 FPD users were not deleted or modified within 51 days after the completion of the 3rd quarter. *Sunflower* During our FY 2010 test work, we determined that the Office of Property Management (OPM) performs monthly access reviews over Sunflower user accounts. OPM runs three Sunflower reports each month, and the Deputy Property Management Officials (DPMOs) and OPM Access Manager review the reports and provide dates and initials by each user reviewed. However, for the three months sampled, we determined that three Sunflower users, who had update privileges, had not had their access removed in a timely manner. All users were reviewed in January, but two were not removed until July, and the other user was not removed until August.	We recommend TSA to take the following corrective actions: CAS/FPD: 1) Have FINCEN update its helpdesk procedures to provide the correct guidelines so that its helpdesk staff will no longer grant additional Standard FPD roles that were not requested on AAR. TSA should closely monitor the requests implemented by FINCEN to ensure that the updated procedures are being followed. 2) Improve the timeline and process of its Quarterly Review. TSA should update its procedures to monitor the timeliness, accuracy and quality of the Quality Review process. a. Update Quarterly Review ISOP to add the expected timeline to complete the quarterly review. b. Conduct timely follow-up and review of the actual FINCEN implementation of the AARs to ensure that the AARs were implemented as requested. 3) Work with FINCEN to identify and implement the best solution to remove the one Sunflower role from the user's profile.		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		4) Work with FINCEN to research and identify options to enhance the automated AAR process. Sunflower: 1) Provide more training and oversight for any new access manager to ensure the process is thoroughly followed. 2) Closely monitor and follow-up with FINCEN to ensure requests are implemented timely and correctly. 3) Review and identify alternate reporting processes in cases of technical difficulties where supervisors cannot access the master files on SharePoint.			
TSA-IT-10-03	During our FY 2010 audit test work, we selected a sample of the following forms required by the TSA directive and determined the following: • Form 1403 Computer Access Agreement: Per the TSA IT Security Policy Handbook, all TSA personnel, including contractors, are required to review and sign Form 1403: Computer Access Agreement upon commencement of working for the agency. Our testing noted that of the five forms sampled, one form was completed one month after the user was granted access to a TSA system.	We recommend that TSA take the following corrective action: Supervisors and Contracting Officer's Technical Representatives within each program office in TSA should ensure, as required by the IT Security Policy Handbook, that evidence be maintained on file for each TSA employee and contractor the Computer Access Agreement form, signed prior to any financial system access is granted.		X	1
TSA-IT-10-04	During the FY 2010 IT audit, we determined that TSA has fully implemented the TSA ISOP: Process for Validation of	We recommend that TSA work with the DHS Chief Financial Officer and the DHS Chief	X		2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	Controls over the USCG Script Process to monitor scripts run at FINCEN. Specifically, we noted that TSA has implemented an extensive review of the scripts that impact TSA on a weekly, monthly, quarterly and ad hoc basis. Additionally, a baseline review was performed to ensure that all scripts that were run in production prior to 4/1/2010. Approximately 160 scripts were reviewed for their purpose and the financial impact of the scripts were understood by the various stakeholders in the script review process, which included the Script Technical Lead, Script Module Leads (SMLs), and Subject Matter Experts (SMEs). Any script that was not included in the baseline review was considered new and was included in the weekly, monthly, quarterly and ad hoc review process. The reviews conducted by TSA included validation and verification steps to ensure that the Coast Guard is properly tracking the TSA scripts and that those scripts go through the proper configuration management processes. We noted no exceptions during our testing of the TSA Script Configuration Management (CM) Oversight Process. <u>Configuration Management Controls Over the Coast Guard Scripting Process</u> The analysis conducted over the Coast Guard script configuration management process reflects the assessment of the control environment for the entire fiscal year. Weaknesses identified over the process are risks that existed in the environment from October 2009 to September 2010 unless otherwise noted.	Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions to: 1) Update the scripting policies and procedures to include additional and more detailed test documentation; 2) Develop training that addresses all aspects of script testing (including documentation of test documents) and provide training to appropriate CM staff; 3) Develop a resource plan (RP) with associated supporting business case(s) to address the database audit logging requirements; 4) Develop procedures and perform regular account revalidation for Serena to ensure privileges remain appropriate; and 5) Conduct an assessment over the ICOFR process related to identifying and evaluating scripts that have a financial statement impact. This assessment can be included in the Configuration Management Oversight Process as part of Coast Guard's annual A-123 efforts or performed independent of the A-123 process. We recommend that this assessment (1) be performed early in the FY 2011, in time to remediate deficiencies before the end of the third quarter, and (2) involve process documentation and sufficient testing to fully			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	1. Based upon follow-up test work performed in FY 2010, we determined that some previously noted weaknesses were remediated (particularly in the second half of FY 2010), while other control deficiencies continued to exist. The remaining control deficiencies that were present throughout FY 2010 vary in significance; however three key areas that impact the Coast Guard Script control environment are: 1) Script Testing Requirements, 2) Script Testing Environment, and 3) Script Audit Logging Process. a. Script Testing Requirements: Limited testing requirements exist to guide FINCEN staff in the development of test plans and guidance over the functional testing that should be performed. Additionally, we determined that there are no detailed requirements over the review and testing of functional changes to the data. FINCEN only tracks and documents the number of transactions updated on scripts that have a financial impact and not the detailed dollar amounts associated with the financial impact transactions. b. Script Testing Environment: Not all script changes were tested in the appropriate CAS Suite test environments as required. FINCEN management informed us that the testing environments, CAS4 and LUFSFQT3, were offline for these exceptions due to a refresh of the databases and that testers used CAS3 and Alpha as alternate testing environments instead.	third quarter, and (2) involve process documentation and sufficient testing to fully assess both design and operating effectiveness of controls. The objective is to have a reliable process and internal controls in place that allow the auditor to test, and rely on those controls, during the fourth quarter of FY 2011. TSA Specific Recommendation: Continue to conduct an assessment over the ICFOR process related to identifying and evaluating scripts that have a financial statement impact. Findings should be communicated and coordinated with USCG, as appropriate. This assessment can be included in the testing of the TSA Script Configuration Management Oversight Process as part of TSA's annual A-123 efforts. Further, we recommend that this assessment (1) be performed early in the FY 2011, in time to remediate deficiencies before the end of the third quarter, and (2) involve process documentation and sufficient testing to fully assess both design and operating effectiveness of controls. The objective is to have a reliable process and internal controls in place that allow the auditor to test, and rely on those controls, during the fourth quarter of FY 2011.			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	However, FINCEN management informed KPMG that these environments are refreshed on an as needed basis and no further information could be provided on how frequently the CAS3 and Alpha databases were refreshed to verify that the scripts were adequately tested in the appropriate environment. Furthermore, we determined that guidance is not provided over the use of alternate testing environments for the testing of scripts to ensure they are adequately tested. c. Script Audit Logging Process: The CAS, FPD, and Sunflower databases are logging changes to tables as well as successful and unsuccessful logins. However, no reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities and ensure that all scripts run have been approved through CMSS or Serena. In addition, we noted that FINCEN has not established a formal process to monitor and review changes made to the Sunflower database including the tables and activities modified by the database administrators. Internal Control Over Financial Reporting – Financial Statement Impact. The USCG has established certain processes to identify and assess the validity of scripts that may have a financial statement impact [on both USCG and TSA financial				

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	statements]. This process is performed by one primary individual, and two identified backup personnel, who perform a review of the script for accuracy and propriety, provides feedback to the source, and ultimately approves the application. This process has certain control deficiencies that have been communicated to USCG (see NFR # CG-IT-10-05), which have led, in part, to TSA's adoption of certain redundant controls to review TSA scripts for propriety. Furthermore, the rationale documenting the impact of the script, whether deemed as having financial impact or not, is not documented and retained. In addition, within the CAS Suite environment, there are over 200 scripts run on a weekly basis. During FY 2010, through this review TSA has discovered various errors that USCG was required to correct. The exceptions noted by TSA are indicative of weaknesses in the USCG process. We also consider this control aspect to be principally important for TSA to monitor Coast Guard's corrective actions taken. In addition, TSA should consider, as part of their annual A-123 efforts, adding their own A-123 testing procedures in identifying and evaluating the financial impact of TSA scripting at the Coast Guard.				

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at TSA

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-10-20	TSA Computer Access Agreement Process		TSA-IT-10-03
TSA-IT-10-23	Configuration Management Controls Over the Coast Guard Scripting Process (Included a specific TSA condition)	X	
TSA-IT-10-28	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		TSA-IT-10-01
TSA-IT-10-29	Core Accounting System, Financial Procurement Desktop , and Sunflower Access Recertifications		TSA-IT-10-02

U.S. Department of Homeland Security

Office of Finance and Administration
601 South 12th Street, TSA-14
Arlington, VA 20598-6014
Washington, DC 20528

Transportation Security Administration

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General, Information Technology Audits
Department of Homeland Security
Office of Inspector General
245 Murray Lane, SW
Building 410
Washington, DC 20528

FROM: Dr. Emma Garrison-Alexander 2/10/2011
Dr. Emma Garrison-Alexander
Chief Information Officer
Transportation Security Administration

David Nicholson 2.11.2011
Chief Financial Officer
Office of Finance and Administration

SUBJECT: Response – *Draft Report: Information Technology Management Letter for the Transportation Security Administration Component of the FY 2010 DHS Financial Statement Audit*

Dear Mr. Deffer:

Thank you for the opportunity to comment on the *Draft Report: Information Technology Management Letter for the Transportation Security Administration Component of the FY 2010 DHS Financial Statement Audit.* TSA has reviewed the Management Letter and confirmed the conditions and recommendations are consistent with NFRs received in the FY 2010 audit. We are in the process of implementing the recommendations and have no changes to the draft report. Again, TSA appreciates the opportunity to review the report, and we look forward to working with your team during the upcoming FY 2011 Financial Statement Audit.

File: 1000.2.1-a

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Administrator, TSA
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, TSA
Chief Information Officer, TSA
Chief Information Security Officer
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

• Call our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.