Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2009 Transportation Security Administration Financial Integrated Audit

OIG-10-82

April 2010

Office of Inspector General

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

April 15, 2010

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 2009 Transportation Security Administration (TSA) financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors Report*, dated March 17, 2010 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at TSA in support of the DHS FY 2009 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated April 2, 2009, and the conclusions expressed in it. We do not express opinions on TSA's 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

April 2, 2010

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
Transportation Security Administration

Chief Financial Officer
Transportation Security Administration

Ladies and Gentlemen:

We have audited the consolidated balance sheet of the U.S. Department of Homeland Security (DHS), Transportation Security Administration (TSA) as of September 30, 2009. The objective of our audit was to express an opinion on the fair presentation of this consolidated balance sheet. In connection with our fiscal year 2009 audit, we also considered TSA's internal controls over financial reporting, and tested TSA's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the consolidated balance sheet. To assist in planning and performing the audit we performed an evaluation of information technology general controls (ITGC). The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is further described in Appendix A.

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 over financial reporting 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 over financial reporting, 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.

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 IT general controls which we believe contribute to a DHS-level significant deficiency and that is considered a significant deficiency in IT controls and financial system functionality. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

The significant deficiency described above is presented in our *Independent Auditors' Report*, dated March 17, 2010. This letter represents the separate restricted distribution report mentioned in that report.

The significant deficiency and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR). We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. 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. In addition, we have provided: a description of key ***TSA*** financial systems and IT infrastructure within the scope of the FY 2009 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated March 23, 2010. TSA's response to the findings identified is attached to this letter. We did not audit TSA's response, and accordingly, we express no opinion on it.

This report is intended solely for the information and use of DHS 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

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2009

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

We have audited the Transportation Security Administration's (TSA) consolidated balance sheet as of September 30, 2009. In connection with our audit of TSA's consolidated balance sheet we performed an evaluation of information technology general controls (ITGC), to assist in planning and performing our audit. The U.S. Coast Guard's Finance Center (FINCEN) hosts key financial applications for TSA. As such, our audit procedures over information technology (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 Government Accountability Office (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.

- *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.
- *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.
- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-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, 2009 due to the nature of prior-year audit findings.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2009, TSA took corrective action to address prior year IT control deficiencies. For example, TSA made improvements in providing IT security awareness training and developing policies and procedures over their own configuration management monitoring controls. However, during FY 2009, we continued to identify IT general control deficiencies that impact TSA's financial data. The most significant issues from a financial statement audit perspective related to controls over the development, implementation, and tracking of scripts at Coast Guard's FINCEN. Collectively, the IT control deficiencies limited TSA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted the internal controls over TSA financial reporting and its operation and we consider them to collectively represent a significant deficiency for TSA under standards established by the American Institute of Certified Public Accountants (AICPA). 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 4 findings issued during our TSA FY 2009 testing, 2 were repeated findings and 2 were new IT findings. These findings represent deficiencies in three of the five FISCAM key control areas. Specifically the deficiencies were: 1) monitoring controls over the scripting process that are not fully designed and operating effectively, 2) unverified access controls through the lack of comprehensive user access privilege re-certifications, and 3) security management issues involving the terminated employee process.

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) unverified access controls through the lack of user access privilege re-certifications, 3) security management issues involving civilian and contractor background investigations, 4) physical security and security awareness issues, and 5) procedures for role-based training for individuals with elevated responsibilities not fully defined. 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 CONTROL AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS BY AUDIT AREA

Findings Contributing to a Significant Deficiency in IT at the TSA Level

Conditions: In FY 2009, the following IT general control and financial system functionality deficiencies were identified at TSA and Coast Guard and contribute to a DHS-level significant deficiency that is considered a significant deficiency in IT general and application controls for TSA. Our findings are divided into two groupings: 1) IT general controls and 2) Financial system functionality.

Related to IT General Controls

IT General Controls: Configuration Management – we noted:

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 to its core general ledger software as necessary to process financial data. However, the Coast Guard has not fully developed testing standards to guide staff in the development and functional testing of IT scripts, documented policies and procedures over testing plans that must be performed, and improve processes to ensure that all necessary approvals are obtained prior to implementation. Specifically, we noted the following Coast Guard design issues, operating effectiveness deficiencies, as well as TSA's own monitoring deficiencies associated with the IT script control process:

- Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests.
- FINCEN analysts may run scripts without seeking further approval from the functional supervisors for approved recurring scripts.
- Testing requirements are inconsistently followed for the testing of the recurring approval scripts and retaining evidence of testing.
- No reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities using this report as it is too difficult to accurately and effectively reconcile the scripts to the audit log table changes.
- The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts.
- Variations in the way the PRP approval forms are populated and completed exist for fields such as financial impact, test strategy and baseline determinations.
- Proper approval is not consistently obtained and documented prior to the running of each script.

Related to financial system functionality:

We noted that financial system functionality limitations are contributing to control deficiencies and inhibiting progress on corrective actions for Coast Guard. These functionality limitations are preventing the Coast Guard 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 IT scripts. The IT script process was instituted as a solution primarily to compensate for system functionality and data quality issues; and
- Annual financial system account recertifications are not being performed due to limitations in the systems.

Recommendations: Unless specifically noted where TSA needs to take specific corrective action, we recommend that the TSA CFO and CIO work with the DHS Office of Chief Information Officer (OCIO) to ensure that the Coast Guard/FINCEN complete the following corrective actions:

- Continue to design, document, implement, and enforce the effectiveness of internal controls associated with the active (current and future) scripts;
- Update / develop procedures and implement technical controls in the CAS and FPD databases to ensure that the appropriate monitoring and review of script activities is performed and documented;
- Continue to update script policies and procedures to include clear requirements and more detailed guidance over requesting recurring scripts, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. Additionally, ensure that the policies and procedures include detailed guidance over the requirements for the testing of scripts and associated test plans to ensure that the appropriate financial impact of the script is evaluated, reviewed by the appropriate personnel, tested in an appropriate test environment prior to being put into production, and documented prior to execution;
- Further develop and implement policies and procedures governing the script change control process to ensure that all script records within the CMSS are accurate and complete; and
- Address the IT system aspects associated with the financial system functionality issues listed in bullets No. 1 and No. 2 above, or develop compensating/mitigating controls in order to eliminate or reduce the associated risk.

TSA Specific Recommendation:

We recommend that the TSA CFO and CIO continue to develop and implement monitoring controls over the FINCEN IT scripting process for the scripts that impact TSA. Additionally, the CFO and CIO should ensure that the TSA policies and procedures include detailed guidance over the requirements for TSA's own monitoring and review of the scripts, including associated test plans to ensure that the appropriate TSA financial impact of the script is evaluated and reviewed by the appropriate personnel, tested in an appropriate environment prior to being put into production, and documented prior to execution.

In addition, we recommend that TSA CFO and CIO obtain the results of the study performed by an outside contractor in FY 2009 and determine if any findings and recommendations should be considered to strengthen internal controls.

Other Findings in IT General Controls

In addition to the configuration management and financial system functionality issues mentioned above, the following deficiencies were also identified during our TSA IT engagement:

Access controls – we noted:

- 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 – we noted:

- 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.

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	4
For Official Use Only (FOUO)	0
Keys/Badges	0
Personally Identifiable Information (PII)	0
Server Names/IP Addresses	0
Laptops	0
External Drives	0
Credit Cards	0
Classified Documents	0
Other –US government official passport	0
Total Exceptions at TSA HQ	**4**

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
20	5	0 Passwords Provided

Recommendations: We recommend that TSACFO and CIO take the following corrective actions:

For access controls:

- Update the quarterly review process to include procedures surrounding the recertification of accounts with elevated privileges on the Unit Approved Plan. In addition, the recertification process should be documented, include supervisor written approval and occur on an at least annual basis.

For entity-wide security program planning and management:

- Implement the Employee Exit Clearance Procedures by completing, certifying, and maintaining all forms required during the exit process for employees and contractors;
- Implement the IT Security Policy Handbook by verifying that all TSA employees and contractors sign a computer access agreement prior to being granted system access;
- Review its policies and procedures regarding Protection of Sensitive Information and update where required in order to address DHS and other Federal requirements, with emphasis being placed on the potential impacts of not consistently and adequately protecting this sensitive information; and

- Review, and update as required, its security awareness / training content to address the updated Protection of Sensitive Information policies and procedures.

Cause/Effect: Many of these deficiencies were inherited from the Coast Guard's lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS Sensitive System Policy 4300A Directive and Handbook and NIST guidance. The lack of documented and implemented security configuration management controls may result in security responsibilities communicated to system developers improperly as well as the improper implementation and monitoring of system changes by Coast Guard management. This also increases the risk of unsubstantiated changes as well as changes that may introduce errors or data integrity issues that are not easily traceable back to the changes. In addition, it increases the risk of undocumented and unauthorized changes to critical or sensitive information and systems. This may reduce the reliability of information produced by these systems. In addition, reasonable assurance should be provided that financial system user access levels are limited and monitored by both TSA and Coast Guard management for appropriateness and that all user accounts belong to current employees. This is particularly essential for those user accounts that have been identified as having elevated privileges. This may also increase the risk that the confidentiality, integrity, and availability of system controls and the financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements. In addition, without proper personnel security measures in place, such as background investigations, TSA financial data could be inappropriately manipulated by contract personnel whose intent is to create havoc or inappropriate financial gain.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition, OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

APPLICATION CONTROLS

Application controls were not tested for the year ending September 30, 2009 due to the nature of the current year's audit findings.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from TSA's Chief Financial Officer. Generally, the TSA management agreed with all of 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, 2009

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2009 TSA Integrated Audit at the Transportation Security Administration

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2009

Below is a description of significant TSA financial management systems and supporting Information Technology (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 Finance Center (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 the Coast Guard. 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 (COTS) product hosted at FINCEN and used for TSA and Federal Air Marshals (FAMS) property management. Sunflower interacts directly with the FA module in CAS. Additionally, Sunflower is interconnected to the FPD system.

Appendix B

FY2009 Notice of IT Findings and Recommendations at the Transportation Security Administration

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2009

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 the Transportation Security Administration 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, 2009

Department of Homeland Security
Transportation Security Administration
FY2009 Information Technology
Notice of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating**
TSA-IT-09-20	We were unable to obtain 6 of the 8 Employee Exit Clearance Forms and 1 of the 3 Separating Non-Screener Employee and Contractor IT Certificates sampled.	• Complete workgroup efforts to establish clear ownership and corrective action plans for the conditions noted. • Complete and maintain all forms during the exit process, as required by the Employee Exit Clearance procedures for employees and contractors. • Verify that a computer access agreement is acknowledged by all TSA employees and contractors, as required by the IT Security Policy Handbook, and that evidence of this acknowledgement is maintained.		X	1
TSA-IT-09-23	Deficiencies continued to exist over the script configuration management process. Specifically, Deficiencies were noted in the areas of approvals, testing, monitoring, maintaining documentation, and audit logging. • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests. • Coast Guard Finance Center (FINCEN) analysts may run scripts without seeking further approval from the Functional Supervisors for approved recurring scripts. • Testing requirements are inconsistently	Continue making improvements to implement and better document an integrated script configuration management process that includes enforced responsibilities of all participants in the process, and the continued development of documentation requirements. We recommend that the Coast Guard should: • Continue to design, document, implement, and enforce the effectiveness of internal controls associated with the active (current and future) scripts. With respect to procedures already in place, Coast Guard should:		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating**
	followed for the testing of the Recurring Approval scripts and retaining evidence of testing. • No reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities using this report as it is too difficult to accurately and effectively reconcile the scripts to the audit log table changes. • The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts. • Variations in the way the Production Review Process (PRP) Approval Forms are populated and completed exist for fields such as financial impact, test strategy and baseline determinations. • Proper approval is not consistently obtained and documented prior to the running of each script. In addition, we noted the following deficiencies related to TSA monitoring controls over the Coast Guard IT script process: • TSA management receives a weekly script report as well as a Validation of Monthly Recurring Scripts from FINCEN. However, we were informed that TSA was still requesting modifications to the script	• Update / Develop procedures and implement technical controls in the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) databases to ensure that the appropriate monitoring and review of script activities is performed and documented. • Continue to update script policies and procedures to include clear requirements and more detailed guidance over requesting recurring scripts, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. Additionally, ensure that the policies and procedures include detailed guidance over the requirements for the testing of scripts and associated test plans to ensure that the appropriate financial impact of the script is evaluated, reviewed by the appropriate personnel, tested in an appropriate test environment prior to being put into production, and documented prior to execution. • Further develop and implement policies and procedures governing the script change control process to ensure that all script records within the Change Management Script System are accurate and complete.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating**
	reports and had asked FINCEN to go back into Change Management Script System (CMSS) to populate missing information so that further analysis could be conducted. Additionally, during test work, we noted that for eight PRP forms, the financial impact determination did not match the CMSS script record field. • TSA management is still in the process of identifying the appropriate subject matter experts in each area and have not formalized the roles and responsibilities surrounding this process. • TSA policies and procedures developed by require that the TSA subject matter experts utilize the financial impact guidance set forth by FINCEN management in the PRP Staff Instruction. However, upon inspection of the PRP Instruction we determined that this guidance does not adequately include detailed criteria to determine financial impact. • Once the financial impact is assessed and approved by FINCEN for the parent blanket approved recurring script, the testing of the script is not subsequently reviewed by an individual with financial reporting knowledge for child scripts that are run in production to ensure that financial impact is correct before the script is placed in production. • TSA is not asked to review and approve all scripts with a financial impact – thus a				

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating**
	Coast Guard approver may approve a script that TSA is not in agreement with, or even aware of.				
TSA-IT-09-28	During our after-hours physical security testing, we identified 4 passwords located on employee workstations.	Review security awareness programs designed to protect financial data to help ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical TSA financial data and hardware that supports financial data.	X		1
TSA-IT-09-29	Controls over the TSA quarterly access reviews for CAS and FPD user accounts have not been effectively implemented to ensure that TSA users who no longer require system access are removed in a timely manner.	Develop and effectively implement quarterly review policies and procedures that include follow-up measures that will be enforced to ensure that users identified through these reviews are maintaining unnecessary access have their accounts end dated in a timely manner.	X		1

Appendix C

Status of Prior Year Notices of Findings and Recommendations And Comparison To Current Year Notices of Findings and Recommendations

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-08-01	The Coast Guard Finance Center (FINCEN) Continuity of Operations Plan (COOP) has not been updated to reflect the results of testing the COOP, and the Business Continuity Plans for each division have not been finalized.	X	
TSA-IT-08-03	During the first half of the fiscal year, the contract with the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) software vendor was still in place, and no corrective action had taken place related to the prior year recommendation. Therefore, the risk exists that the condition was present for the majority of the fiscal year. However, due to the Coast Guard decision to terminate the contract with their software vendor and the Coast Guard Headquarters decision to suspend all Software Problem Reports (SPRs) and Software Change Requests (SCRs), the condition did not exist beyond the date of these 2 events.	X	
TSA-IT-08-05	Coast Guard Headquarters has developed but not yet implemented policies and procedures to require that a favorably adjudicated background investigation be completed for all contractor personnel. **(1)**	X	
TSA-IT-08-06	Coast Guard headquarters has not finalized the Role-Based Training for Coast Guard Information Assurance Professionals Commandant Instruction, which will require all Coast Guard members, employees, and contractors with significant IT security responsibilities to receive initial specialized training and annual refresher training thereafter. The online Training Management Tool, which will track compliance, will not be implemented until the Role-Based Training is implemented. **(1)**	X	
TSA-IT-08-13	FINCEN has not completed the risk assessment for the CAS Suite, and the CAS System Security Plan (SSP) is still in draft form.	X	
TSA-IT-08-15	Of the 669 employees/contractors with current access to the following TSA's financial applications: CAS, FPD, and Sunflower; 152 employees/contractors have not completed the IT Security Awareness Training.	X	
TSA-IT-08-18	Configuration management deficiencies continue to exist on hosts supporting the CAS, FPD and WINS applications and the underlying General Support Systems (GSS). Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions.	X	
TSA-IT-08-19	Security patch management deficiencies continue to exist on hosts supporting the CAS, FPD and WINS applications and GSS. Note: Due to the nature of this testing, see the tables in the NFR	X	

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	for the specific conditions.		
TSA-IT-08-20	We were unable to obtain 21 1163 Forms and 27 1402 Forms for each sample of 40. Additionally, 2 of the 13 1402 Forms received were signed after the forms were requested for audit. The IT Security Policy Handbook requires all TSA personnel including contractors to review and sign the TSA Form 1403: Computer Access Agreement. However, we were unable to obtain 7 of the 25, 1403: *Computer Access Agreements* sampled. Of the 18 forms we obtained, 5 were dated after the sample was requested for audit.		09-20
TSA-IT-08-21	The change control policy has not been fully completed and implemented. The United States Coast Guard (CG) is responsible for making software changes to the CAS, FPD and Sunflower applications, however, on March 31, 2008, CG HQ terminated its contract with the software vendor/developer for CAS, FPD and Sunflower, which has hindered TSA's ability to fully complete and implement the CAS, FPD and Sunflower change control policy.	X	
TSA-IT-08-22	We noted that control deficiencies still exist within the design of FINCEN's Configuration Management policies and procedures for CAS and FPD, as well as the operating effectiveness of those controls. Our test work over the design of the change controls covered both periods of the change control environment; however, our testing of operating effectiveness covered only the period of start of the fiscal year through March 2008, since no changes were made to CAS and FPD from April through the remainder of the fiscal year.	X	
TSA-IT-08-23	Coast Guard's controls over the scripting process remain ineffective. Deficiencies were noted in controls over script implementation, approvals and testing, as well as active script modification. In addition, Coast Guard has not maintained or developed a population of scripts run since the inception of CAS in 2003 nor has it performed a historical analysis of script impact on the cumulative balances in permanent accounts of the financial statements. Specifically: • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests; • The Procedures for Data Scripts do not specifically state the testing and documentation requirements for blanket approval scripts and this policy remains in draft form; • Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through SQL		09-23

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	Navigator to run scripts or review what scripts are run; • The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts; and • Coast Guard has not completed PRP documentation for all scripts executed since their implementation. Additionally, although Coast Guard did conduct an examination with an external contractor organization, we have determined that the analysis was incomplete. Specifically, due to the many limitations over scope, it did not consider the full population of scripts run at FINCEN currently or since the inception of CAS. Furthermore, the analysis did not properly evaluate scripts as to financial statement impact, including current versus prior year effect.		
TSA-IT-08-24	Although Coast Guard Headquarters is in the process of completing background investigations for all civilian employees, this has not been completed. Additionally, Coast Guard has set its position sensitivity designations to Low for the majority of its employees. However, DHS requires position sensitivity designations no less than Moderate which equates to a Minimum Background Investigation (MBI). Therefore, we determined that the conditions noted in prior year have not been remediated. **(1)**	X	

(1): The TSA NFRs listed as closed were based upon exceptions identified at Coast Guard from previous years. These NFRs were not closed due to Coast Guard remediating the exceptions during the year, but instead it was determined that they would be closed from a NFR delivery perspective.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2009

U.S. Department of Homeland Security

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

Transportation Security Administration

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

Dear Mr. Deffer:

Thank you for the opportunity to comment on the *Draft Report: Information Technology Management Letter for the FY 2009 Transportation Security Administration (TSA) Financial Integrated Audit*. TSA appreciated your recommendations included in your report and we look forward to working with your team during the upcoming FY 2010 audit.

Sincerely,

David R. Nicholson
Assistant Administrator and Chief Financial Officer
Office of Finance and Administration

File: 1000.2.1-a

www.tsa.gov

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2009

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, Policy
Assistant Secretary for Public Affairs
Assistant Secretary for 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.