DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2007 Transportation Security Administration Balance Sheet Audit (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General has redacted this report for public release. A review under the Freedom of Information Action will be conducted upon request.

OIG-08-72

June 2008

Office of Inspector General

U.S. Department of
Homeland Security
Washington, DC 20528

Homeland
Security

June 27, 2008

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 Transportation Security Administration (TSA) balance sheet audit as of September 30, 2007. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-08-57, May 2008) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of TSA's FY 2007 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated February 8, 2008, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion 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. It is our hope 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

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

February 8, 2008

Chief Financial Officer
Transportation Security Administration

Chief Information Officer
Transportation Security Administration

Inspector General
U.S. Department of Homeland Security

Ladies and Gentlemen:

We have audited the consolidated balance sheet of the U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA) as of September 30, 2007, and have issued our report thereon dated February 8, 2008. In planning and performing our audit of the consolidated balance sheet of TSA, we considered internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing an opinion on the consolidated balance sheet. An audit does not include examining the effectiveness of internal control and does not provide assurance on internal control over financial reporting. We have not considered internal control since the date of our report.

We noted certain matters involving internal control and other operational matters with respect to information technology that are summarized and presented in Exhibit A for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and have been communicated through the issued Notices of Finding and Recommendation, are intended to improve information technology internal control or result in other operating efficiencies; and are intended **For Official Use Only**. Exhibits B – D present additional information for management's use. Exhibit E contains a copy of the written TSA's management response to the draft letter. Our findings involving internal control and other operational matters that do not relate to information technology have been presented in our *Independent Auditors' Report*, dated February 8, 2008, and in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated December 21, 2007.

Our audit procedures are designed primarily to enable us to form an opinion on the consolidated balance sheet, and therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of TSA's organization gained during our work to make comments and suggestions that we hope will be useful to you. We would be pleased to discuss these comments and recommendations with you at any time.

This report is intended solely for the information and use of TSA and DHS management, DHS Office of Inspector General, Office of Management and Budget, 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

Transportation Security Administration
Information Technology Management Letter
For the FY 2007 TSA Balance Sheet Audit

INFORMATION TECHNOLOGY MANAGEMENT LETTER

Table of Contents

Transportation Security Administration
Information Technology Management Letter
For the FY 2007 TSA Balance Sheet Audit

Exhibit A

OBJECTIVE, SCOPE AND APPROACH

We performed audit procedures over the U.S. Department of Homeland Security's (DHS) Transportation Security Administration's (TSA) general controls in support of the fiscal year 2007 TSA balance sheet audit. The overall objective of our audit procedures was to evaluate the effectiveness of information technology (IT) general controls of TSA's financial processing environment and related IT infrastructure as necessary to support the engagement. Further information related to the scope of the TSA's IT general controls assessment is described in Exhibit B. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office, formed the basis of our audit procedures.

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 six control functions to be essential to the effective operation of the general IT controls environment.

- *Entity-wide security program planning and management* – 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* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Application software development and change control* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software* – Controls that limit and monitor access to powerful programs that operate computer hardware.
- *Segregation of duties* – 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.
- *Service continuity* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

In addition, we assessed the DHS component's compliance with the National Institute of Standards and Technology's (NIST) *Special Publication, 800-53, Recommended Security Controls for Federal Information Systems* and DHS' *Information Technology Security Program Publication, 4300A*.

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

In addition to testing TSA's general control environment, we performed application control tests on a limited number of TSA financial systems and applications. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

Exhibit A

- *Application Controls* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

The U.S. Coast Guard's [redacted] [redacted] 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 [redacted] policies, procedures, and practices, as well as at TSA Headquarters.

During fiscal year 2007, there were ten TSA prior year findings that were properly closed. During the year, the [redacted] took steps to address known weaknesses, such as expanding password lengths on key financial systems and taking steps to improve the service continuity processes.

Despite these improvements, during our current year test work, we noted that 14 prior year findings had not been resolved, and we issued 11 new findings. These issues collectively limit TSA's ability to ensure that critical financial and operational data is maintained in a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over TSA financial reporting and its operation. TSA and Coast Guard management should ensure an emphasis is placed on the monitoring and enforcement of IT security-related policies and procedures. On-going measures to improve the IT security considerations for key financial systems hosted by [redacted] and implement effective access controls and change controls need to be completed. Additionally, many of the repeat vulnerabilities in system access and configuration controls that were identified during technical security testing can be addressed by ensuring that the security configurations associated with the builds, service packs, and software patches are in compliance with DHS and National Institute of Standards and Technology (NIST) standards.

FINDINGS BY AUDIT AREA

Conditions: In fiscal year 2007, the following IT and financial system control weaknesses were identified at TSA and at [redacted]. Many of the issues identified during our fiscal year 2007 engagement were also identified during fiscal year 2006. The following IT and financial system control weaknesses result in IT being reported as a material weakness.

A. Access Controls

Access controls for general support systems and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, loss, or impairment. Access controls are facilitated by an organization's entity-wide security program. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of information.

Transportation Security Administration
Information Technology Management Letter
For the FY 2007 TSA Balance Sheet Audit

Exhibit A

During fiscal year 2007, we noted that [redacted] had made progress toward the improvement of access controls surrounding the financial applications by expanding password lengths on key financial systems, improving the personnel entrance and exit procedures, and improving control access over the [redacted] operating system environment. However, we also noted several repeat access control weaknesses in addition to the identification of several new weaknesses. The weaknesses were identified as a result of general controls and vulnerability testing. These are significant issues because personnel inside the organization who best understand the organization's systems, applications, and business processes are able to obtain unauthorized access to TSA data.

Conditions noted during our test work at [redacted] and TSA Headquarters regarding access controls that impact TSA's financial processing are as follows:

- Missing or weak user passwords were identified on key servers and databases that process and support TSA financial data.
- Excessive administrative privileges were identified on the [redacted].
- Certain workstations, servers, and network devices were not configured with the necessary security patches, or were not configured in the most secure manner.
- Accounts of terminated employees and contractors are not removed from [redacted] in a timely manner.
- Procedures for the authorization, regular review, and removal of [redacted] system access were not formalized and were inconsistent.
- The [redacted] and [redacted] have been configured to automatically end date accounts that have not been used in six months; however, DHS guidance requires accounts that have been inactive for 30 days be disabled.
- Policy and procedures for a formalized sanctioning process for individuals who do not follow computer access policies and procedures have not been fully developed and implemented. Specifically, the policies and procedures do not include consequences for individuals who do not sign the computer access agreements or complete initial or refresher security awareness training. Furthermore, of the nine individuals selected for testing, only one had completed a computer access agreement.
- Procedures requiring the review of the activities of [redacted] system administrators are not formally documented.
- Audit logging has not been enabled with in the [redacted] system. Additionally, audit trails of appropriate user actions, including changes to security profiles, are not generated and maintained for certain applications.

Recommendation:

We recommend that the TSA Chief Financial Office (CFO) and Chief Information Officer (CIO) ensure the following corrective actions are implemented:

1. **Enforce password controls that meet DHS password requirements on key financial systems.**
2. **Remove all generic shared system accounts or establish individual accountability for these accounts. If these accounts cannot be removed, enable audit logging to capture the user's operating system logon ID so that individual accountability can be established for each instance of when these accounts are used *(TSA needs to take part of this action)*.**

Exhibit A

3. Develop and implement a process for performing scans of the network environment, including the financial processing environment, for the identification and correction of vulnerabilities in accordance with DHS and Federal guidance. These scans should occur on a regular basis, especially after the implementation of a software release.
4. Track and end-date/disable inactive and/or separated personnel [redacted] accounts in compliance with DHS requirements.
5. Develop and implement formal entity-wide procedures for controlling the processes associated with the granting, monitoring, and terminating user accounts that require the periodic revalidation of user profiles by local security administrators that comply with existing policies *(TSA needs to take this action).*
6. Ensure that computer access agreements are completed for all TSA employees and contractors with access to financial applications (*TSA needs to take this action*).
7. Continue the development and implementation of a sanctioning process for both TSA employees and contractors if requirements surrounding the completion of security awareness and training, and computer access agreements are not met.
8. Establish detailed procedures for audit trail generation, review and management on the [redacted] system accounts. The procedures should discuss the conditions under which the audit trails should be generated and reviewed, the frequency of the reviews, and the basis for determining when suspicious activity should be investigated. In addition, sufficient resources should be allocated to ensure the proper implementation and monitoring of these procedures.

B. Application Software Development and Change Control

Conditions noted during our test work at [redacted] and TSA Headquarters regarding the change control process that impact TSA's financial processing are as follows:

- Several weaknesses exist in the change control processes for [redacted]. Specifically, change control procedures were not properly developed, formal change request forms were not in use, and test plans and results were not documented.
- A separate and secondary change control process outside of and conflicting with the established change control process is in operation at the [redacted]. Specifically, this second change control process is used to create additional functionality or correct data in [redacted] to compensate for gaps in the customized software. During our testing of this separate process, we identified it to be informal, undocumented, and not effective.

Recommendation:

We recommend that the TSA CFO and CIO ensure the following corrective actions are implemented:

1. Develop and enforce a standard set of configuration management procedures for developing and documenting test plans, documenting test results, delivering and implementing software, and management approving system changes for normal and emergency upgrade situations.
2. Implement a single, integrated change control process over the Coast Guards' financial systems with appropriate internal controls to include clear lines of authority to the components' financial management personnel and to enforce responsibilities of all participants in the process and documentation requirements.

Exhibit A

C. Entity-Wide Security Program Planning and Management

During fiscal year 2007, we noted continued weaknesses in the area of entity-wide security program planning and management at both [redacted] and at TSA Headquarters. Specifically, conditions noted that impact TSA's financial processing are as follows:

- The contract that Coast Guard Headquarters has with its software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, system builds and maintenance packs may not be configured and implemented with comprehensive security configuration requirements.
- Background investigations of [redacted] civilian and contractors employed to operate, manage and provide security over IT systems are not being consistently conducted.
- TSA allows individuals to complete security awareness training within 60 days of beginning work and gaining access to their local area network (LAN) and application accounts. However, DHS guidance requires that all individuals complete security awareness training prior to gaining access to the information systems. Furthermore, of our sample of nine individuals for testing, one contractor had not completed initial security awareness training this fiscal year and a second employee had not completed the refresher training for this fiscal year.
- Eleven of a sample of 30 TSA 1402 forms, *Separating Non-Screener Employee and Contractor IT Certificates*, were received. Additionally, of the 11 received, seven of the forms did not have the appropriate TSA application(s) identified in order to deactivate the separating employee's accounts. Furthermore, we selected 30 TSA 1163 forms, *the Employee Exit Clearance form,* for both contractors and TSA personnel and only received nine completed forms.
- Coast Guard IT security role-based training policies and procedures lack appropriate criteria for defining personnel with significant IT responsibilities. Additionally, the personnel that are defined in the policy are very limited and do not fully cover the scope of security responsibilities addressed in DHS requirements.
- The Certification and Accreditation (C&A) package of a key system was not complete and in accordance with DHS requirements.

Recommendation:

We recommend that the TSA CFO and CIO ensure the following corrective actions are implemented:

1. Reevaluate and revise the contract between Coast Guard and its software vendor or otherwise ensure that the security configurations associated with the builds, service packs, and software patches are in compliance with DHS and NIST standards.
2. Enforce DHS policy to ensure that all [redacted] contractors and employees go through the appropriate background/suitability check.
3. Enforce the DHS policy by having all new and existing users and contractors complete the security awareness training.
4. Ensure that TSA employees consistently complete the required paperwork for terminated personnel.
5. Enhance current policies and procedures for IT role-based training to require those with critical security responsibilities, such as network administrators, system administrators, senior managers and system owners, to complete the role-based training on an annual basis and deploy the IT role-based

Exhibit A

training of civilian personnel with critical IT positions down to the Coast Guard component levels for implementation.

6. Update the C&A package to ensure that each subsystem component is fully described in the system security plan, an appropriate security categorization is assigned, and an appropriate set of security controls are identified in accordance with NIST guidance.

D. Service Continuity

During fiscal year 2007, we noted that the Coast Guard has continued to take corrective actions to address prior year weaknesses related to service continuity. Despite these improvements, weaknesses still exist that pose a risk of losing the capability to process, retrieve, and protect information maintained electronically which could impact TSA's ability to accomplish financial processing requirements.

Conditions noted at [redacted] regarding service continuity controls that impact TSA's financial processing are as follows:

- One of the business continuity plans is in draft form and has not been tested.
- A memorandum of understanding (MOU) for business continuity services is currently in draft form.
- Nineteen of 79 individuals who had access to the data center, had not yet completed the emergency response training, as follows:

  - 13 individuals (building owners, property managers and their respective contractors)
  - 4 members of [redacted] Senior Management
  - 2 security guards

- Lastly, we identified four employees, each with 24 hour access to the data center, that had not yet completed the emergency response training as of July 2007. Upon notifying [redacted] of this exception, the four individuals completed the training and [redacted] provided the necessary supporting evidence.

Recommendation:

We recommend that the TSA CFO and CIO ensure the following corrective actions are implemented:

1. **Finalize and implement the Continuity of Operations Plan (COOP) and ensure that it addresses disaster recovery procedures.**
2. **Periodically test the business continuity plan and evaluate the results so that the plan can be adjusted to correct any deficiencies identified during testing.**
3. **Finalize the MOU for business continuity services and document associated restoration procedures so that a specific Coast Guard component can serve as an alternate processing site in the event that the [redacted] is unavailable.**
4. **Ensure that all personnel with access to the data center have completed the data center emergency response training.**

Exhibit A

E. System Software

We did not identify any findings in the area of system software during the fiscal year 2007 TSA balance sheet audit.

F. Segregation of Duties

We did not identify any findings in the area of segregation of duties during the fiscal year 2007 TSA balance sheet audit.

G. Application Control Findings

We did not identify any findings in the area of application controls during the fiscal year 2007 TSA balance sheet audit.

Exhibit A

TSA's Management Response and OIG Evaluation

We obtained written comments on a draft of this letter from the TSA CFO and CIO. We have included TSA's written comments in Exhibit E of this letter.

The OIG agrees with the steps that TSA is taking to satisfy these recommendations.

Exhibit B

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE WITHIN THE SCOPE OF THE FY 2007 TSA BALANCE SHEET AUDIT

Below is a description of significant TSA financial management systems and supporting information technology (IT) infrastructure included in the scope of the fiscal year 2007 balance sheet audit.

Locations of Audit: TSA Headquarters in [redacted] and the Coast Guard [redacted]. TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Audit:

- [redacted] – [redacted] is the [redacted] that records financial transactions and generates financial statements for the Coast Guard. [redacted] is hosted at [redacted] in [redacted]. [redacted] interfaces with the [redacted] Additionally, [redacted] fixed asset (FA) module for property management is interconnected to the [redacted] system that is hosted at [redacted].
- [redacted] – The [redacted] application used to create and post obligations to the [redacted]. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. [redacted] is interconnected with the [redacted] systems and is located at the [redacted].
- [redacted]: [redacted] is a customized third party commercial off the shelf (COTS) product used for TSA and [redacted] property management. [redacted] interacts directly with the FA module in [redacted]. Additionally, [redacted] is interconnected to the [redacted] system.

Exhibit C

FY 2007 TSA IT NOTICES OF FINDING AND RECOMMENDATION

Notices of Finding and Recommendation – Definition of Risk Ratings:

The Notice of Findings and Recommendations (NFR) were risk ranked as High, Medium, and Low based upon the potential impact that each weakness could have on the DHS component's control environment and on the integrity of the financial data residing on the DHS component's financial systems. In addition, analysis was conducted collectively on all the NFRs to assess connections between individual NFRs, which when joined together could lead to a control weakness occurring with more likelihood and/or higher impact potential.

High Risk: A control weakness serious in nature to create a potential material misstatement to the financial statements.

Medium Risk: A control weakness, in conjunction with other events, less severe in nature than a high risk issue, which could lead to a misstatement to the financial statements.

Low Risk: A control weakness minimal in impact to the financial statements.

The risk ratings included in this report are intended solely to assist management in prioritizing its corrective actions.

Exhibit C

FY 2007 TSA IT NOTICES OF FINDING AND RECOMMENDATION

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT 07-01	The business Contingency and Disaster Recovery Plan (DRBC) is in draft form and has not been tested for [redacted] and [redacted]. Additionally [redacted] has drafted a memorandum of understanding (MOU) with the [redacted] for reciprocal services; however, the MOU is currently in draft form.	TSA ensure that [redacted] complete the following: 1. Finalize and implement the COOP and ensure that it addresses disaster recovery procedures for [redacted] and [redacted]. 2. Finalize the MOU with the [redacted] and document associated restoration procedures so that the [redacted] can serve as an alternate processing site in the event that the [redacted] is unavailable. 3. Periodically test the COOP and evaluate the results of the testwork so that the COOP can be adjusted to correct any deficiencies identified during testing.		X	Medium
TSA-IT-07-02	The business Contingency and Disaster Recovery Plan (DRBC) is in draft form and has not been tested for the [redacted] Application. Additionally, [redacted] has drafted a memorandum of understanding (MOU) with the [redacted] for reciprocal services; however, the MOU is currently in draft form.	TSA ensure that [redacted] complete the following: 1. Finalize and implement the COOP ensuring it addresses disaster recovery procedures for [redacted] as well as testing the COOP periodically, evaluating the results of the test work so the COOP can be adjusted to correct any deficiencies identified during testing. 2. Finalize the MOU with the [redacted] and document associated restoration procedures so that the [redacted] can serve as an alternate processing site in the event that the [redacted] is unavailable.	X		Medium

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-03	The contract that CG HQ has with the [redacted], [redacted] and [redacted] software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, [redacted], [redacted] and [redacted] builds and maintenance packs may not be configured and implemented with comprehensive security configuration requirements. CG recognizes the absence of security requirements and indicated that the contract with the vendor will be reassessed in 2008 during the contract renewal process with CG HQ and corrective actions will be taken at that time.	TSA should ensure that CG reevaluates and revises the contract between CG and their software vendor or otherwise ensure that the security configurations associated with the builds, service packs, and software patches are in compliance with DHS and NIST standards for [redacted] and [redacted].	X		High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-04	Although [redacted] has developed re-entry procedures, continued to limit entry into the data center and created a curriculum that must be completed annually by data center staff, weaknesses were noted in the process. Specifically, we determined that 19 individuals, specified below, had 24 hour a day access to the data center and had not yet completed the training: - 13 individuals (building owners, property managers and their respective contractors) - 4 members of [redacted] Senior Management - 2 security guards Lastly, we identified four employees, each with 24 hour access to the data center that had not yet completed the training as of July 2007. Upon notifying [redacted] of this exception, the four individuals completed the training and [redacted] provided KPMG with supporting evidence.	We recommend that TSA monitor [redacted] efforts to implement corrective action to ensure that all personnel with access to the data center have completed the data center emergency response training.		X	Low

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-05	No formal procedures have been developed or implemented by Coast Guard Headquarters to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. DHS directives and policies require Coast Guard and other DHS components to ensure the completion of background investigations for all contractors accessing IT systems. The type of background investigations should be based on the risk level of their future position at CG and are required to be completed prior to the start of work. However, no CG guidance exists to require CG components to clear their contractors for suitability, especially those with sensitive IT positions.	TSA should monitor CG's completion of the following corrective actions: 1. Implement procedures to ensure compliance with DHS policies for the background investigations of contracting personnel, such as DHS 4300A. 2. Ensure that all contracts procured by CG HQ, include the appropriate suitability designation for contracting personnel working on the contract and require completion of suitability checks specific to the position risk level prior to beginning work at Coast Guard. Additionally, ensure that all current contracts are updated with the required language. 3. Provide resources to Coast Guard Components to fully implement the developed procedures.		X	High
TSA-IT-07-06	CG IT Security Awareness Policies and Procedures lack appropriate criteria for defining personnel with significant IT responsibilities. Additionally, the personnel that are defined in the guidance are very limited and do not fully cover the scope of security responsibilities addressed in DHS requirements.	TSA should monitor CG's completion of the following corrective actions: 1. Enhance current policies and procedures for IT role based training to require those with critical security responsibilities, such as network administrators, system administrators, senior managers and system owners, to complete the role based training on an annual basis. 2. Deploy the IT role-based training of civilian personnel with critical IT positions down to the CG component levels for implementation.	X		Low

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-07	The following access control weakness surrounding [redacted] were identified: • TSA management did not receive a response from the Federal Air Marshalls Service ([redacted]) Division [redacted] user base for the May and for the July 2007 [redacted] review. Therefore, TSA assumed that no response indicated that all roles were appropriate and did not follow-up to ensure that a response was received. • Privileges associated with each user were not included in the May and July 2007 reviews performed. Additionally, the accounts of terminated employees are not removed from the system in a timely manner. Although TSA requested that several of the accounts of terminated individuals be deactivated/end-dated by [redacted] the requests were not submitted to [redacted] until months after the employees departed and we were unable to obtain evidence that these accounts had in fact been deactivated/end-dated.	TSA should complete the following: 1. Update the [redacted] policies and procedures to require that the privileges associated with each [redacted] user be included in each [redacted] access review. 2. Update the [redacted] policies and procedures to include steps to be followed in the event that a region or a division (such as [redacted]) does not respond to the [redacted] access review request. 3. Notify and coordinate with [redacted] to implement the corrective actions that result from the [redacted] review, such as removing separated users from the system or modifying account privileges in a timely manner and in accordance with DHS guidance.		X	Medium

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-08	The following access control weakness surrounding [redacted] were identified: 1. The [redacted] application and database does not meet the password requirements noted in DHS 4300A. 2. [redacted] accounts of terminated individuals are not removed in a timely manner including one individual who had user account management capabilities within the system. 3. [redacted] application and database accounts are not being reviewed for appropriateness.	TSA should monitor [redacted] completion of the following: 1. Ensure that the [redacted] password configuration meets DHS requirements. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords 2. Remove/end-date/disable the accounts of terminated individuals, both employees and contractors, from the system immediately upon their departure. 3. Develop and implement access control procedures for the [redacted] system and database accounts. These procedures should include, at a minimum, parties involved in the review, steps for reviewing the system and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary.		X	Medium
TSA-IT-07-09	The following access control weakness surrounding [redacted] were identified: 1. We were unable to obtain a copy of the [redacted] password configuration. However, we performed a demonstration/walkthrough of the password with a [redacted] point of contact and was able to determine that the password configuration is not in compliance with DHS guidance. 2. Although the [redacted] system has been configured to track and lock accounts that have not been utilized in 90 days, DHS guidance requires that accounts that have not been used in 30 days be deactivated.	TSA should monitor CG's completion of the following: 1. Configure the [redacted] password configuration to be in compliance with DHS guidance. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc). 2. Configure the system to track and lock inactive [redacted] accounts in compliance with DHS requirements.		X	Medium

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-10	An excessive number of individuals had user administration capabilities within [redacted] until the implementation of the centralized user management. Specifically, 78 individuals had [redacted] account management capabilities within the system. The privileges associated with these accounts permitted the user to create/delete/modify [redacted] user accounts for all of TSA including sites/locations that he/she was not responsible for. Thirteen of these accounts were end-dated (disabled) throughout the FY 2007 period; however, many of these individuals are part of the Financial Systems Branch and should not have such capabilities within the system. [redacted] became responsible for account creation/deletion/modification when the centralized user management was implemented. This effort reduced the number of individuals with account management capabilities to 16. However, we also noted the existence of two shared generic accounts with this privilege: [redacted] and [redacted]. These accounts have every privilege within the application, including the ability to create/delete/modify user accounts within [redacted]	TSA should monitor the following corrective action for [redacted]: 1. Remove all generic shared system accounts or establish individual accountability for these accounts. If these accounts cannot be removed, enable audit logging to capture the user's operating system logon ID so that individual accountability can be established for each instance of when these accounts are used. No recommendation required for the [redacted] excessive administrator access that existed from October 1, 2006 through August 19, 2007 as this weakness was remediated with the implementation of centralized user management.	X		High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-11	[redacted] accounts are not immediately disabled upon an employee's termination. Additionally, formalized policies and procedures for the periodic review of the [redacted] accounts do not exist. Lastly, [redacted] access request forms are not consistently completed.	TSA should complete the following: 1. Immediately notify and coordinate with [redacted] when an employee or contractor separates from TSA so that his/her [redacted] account can be end-dated/disabled in a timely manner. 2. Modify the [redacted] Site Administrator Review Procedures to include, steps for reviewing the application and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that the privileges associated with each individual are still authorized and necessary. The procedures should note the parties that should be involved in the review process, the supporting documentation that should be retained, and procedures to notify [redacted] of corrective action that needs to be taken as a result of the review. 3. Complete an AAR or a Financial Systems Access Request Form for each individual requesting access to the [redacted] application or database.		X	Medium

Transportation Security Administration
Information Technology Management Letter
For the FY 2007 TSA Balance Sheet Audit

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-12	The accounts of terminated contractors are not end-dated or disabled in a timely manner. Additionally, we noted that TSA has not developed policies or procedures that require a periodic review of [redacted] application and database accounts, and their associated privileges, be performed to determine that access is appropriate.	TSA should complete the following: 1. Develop and implement access control policies and procedures for the periodic review of [redacted] application and database accounts for TSA users. These procedures should include, at a minimum, the parties involved, steps for reviewing the application and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that the privileges associated with each individual are still authorized and necessary. 2. Retain supporting documentation associated with the review 3. Notify and coordinate with the [redacted] to implement the corrective actions that result from the review, such as removing separated users from the system or modifying account privileges.		X	Medium
TSA-IT-07-13	[redacted] had not adequately completed the [redacted] Certification and Accreditation (C&A) package to include the [redacted] system. Specifically, [redacted] management stated that [redacted] is a subsystem of [redacted] and a separate C&A does not need to be completed since it is covered by the [redacted] C&A Package. However, we determined that there is no documentation within the [redacted] System Security Plan that defines [redacted] as a subsystem and specifically addresses the appropriate security controls for [redacted] in this capacity.	TSA should monitor [redacted] completion of the following corrective actions: 1. Further define and justify the classification of [redacted] as a subsystem to [redacted] in accordance to NIST guidance. 2. Once recommendation one is complete, update the [redacted] C&A package to include that each subsystem component is fully described in the system security plan, an appropriate security categorization is assigned, and an appropriate set of security controls are identified in accordance with NIST guidance.	X		Medium
TSA-IT-07-14	[redacted] and [redacted] systems have been configured to automatically end date accounts that have not been used in six months; however, DHS guidance requires accounts that have been inactive for 30 days be disabled.	TSA should monitor [redacted] efforts to track and end-date/disable [redacted] and [redacted] accounts in compliance with DHS requirements.	X		Low

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-15	TSA sanctioning policies and procedures have not been fully developed and implemented to include consequences for individuals who do not sign the computer access agreements or complete initial or refresher security awareness training. Additionally, we determined that TSA allows individuals to complete security awareness training within sixty days of beginning work and gaining access to their LAN and application accounts. However DHS guidance requires that all individuals complete security awareness training prior to gaining access to the Information systems. Furthermore, security awareness training and Computer Access Agreements are not consistently completed.	TSA should perform the following corrective action: 1. Review and revise the current TSA policies and procedures for the on-boarding of both contractors and TSA employees according to DHS 4300A and NIST guidance. 2. Continue to develop and implement the policies and procedures for the requirements surrounding the completion of security awareness and training, and computer access agreements for both TSA employees and contractors. 3. Address the weakness surrounding the development and implementation of a sanctioning process for both TSA employees and contractors if these requirements are not met.		X	Low
TSA-IT-07-16	Procedures are not formally documented requiring the review of the activities of the [redacted] system administrators. We also noted that reviews of the audit logs that document the actions of [redacted] administrators in the [redacted] operating environment are not being performed.	TSA should monitor [redacted] completion of the development and implementation of detailed procedures requiring the periodic review of [redacted] audit logs for unauthorized and suspicious activity as well as the performance of periodic audit log reviews of the [redacted] operating system.	X		Medium
TSA-IT-07-17	Procedures are not formally documented identifying how change control should be performed when applying system software changes, including software patches, to the [redacted] operating system according to a standard schedule or in an emergency situation.	TSA should monitor [redacted] efforts to develop and implement detailed procedures for the performance of standard and emergency system software change controls for the [redacted] operating environment.	X		Medium

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-18	Technical testing identified patch management weaknesses on hosts supporting the [redacted] and [redacted] applications which could allow for a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] and [redacted] data.	TSA should monitor [redacted] completion of corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the software builds created by the CG software developer are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.		X	High
TSA-IT-07-19	Technical testing identified configuration management weaknesses on hosts supporting the [redacted] and [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.	TSA should monitor [redacted] completion of corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the software builds created by the CG software developer are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.		X	High
TSA-IT-07-20	The IT off-boarding process for Non-Screeners and Contractors is not consistently completed for terminated personnel. Specifically, only eleven (11) out of a selection of thirty (30) TSA 1402 Forms, the Separating Non-Screener Employee and Contractor IT Certificates, were received. Additionally, of the eleven received, seven (7) of the forms did not have the appropriate TSA application(s) identified in order to deactivate the separating employee's accounts. Furthermore, we selected thirty (30) TSA 1163 forms, the Employee Exit Clearance form, for both contractors and TSA personnel and only received nine (9) completed forms.	TSA should review the current policies and procedures for the exit process of both TSA contractors and employees and develop corrective action plans to remediate the identified weaknesses according to DHS 4300A and NIST guidance.		X	Medium

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-21	The following weaknesses were identified in the TSA [redacted] and [redacted] change control process: 1. TSA has not fully documented policies and procedures surrounding the change control process for [redacted] to define the overlap in the responsibilities between TSA and [redacted] or guidance for ensuring that changes that are passed/deferred to [redacted] are tested and operate appropriately prior to approval by TSA and implementation into production. 2. Additionally, TSA does not consistently retain documentation associated with the [redacted] and [redacted] changes 3. Policies and procedures for the emergency change control process are not documented.	TSA should complete the following: 1. Continue to develop and implement a more detailed change control policy and procedure to formally define the TSA change control to include different roles and responsibilities that personnel within TSA must complete and include instructions for the monitoring [redacted]. 2. Develop and implement policies and procedures to specifically address the documentation of the testing performed in different phases of testing as well as testing performed by [redacted]. 3. Continue to develop and implement a formalized process for the retention of documentation. 4. Ensure that the policies and procedures developed include the emergency change control process for [redacted] and [redacted].		X	High
TSA-IT-07-22	Policies and procedures for the overall change control process surrounding [redacted] and [redacted] changes and emergency changes are inadequate. Specifically procedures detail the overall process and phases for [redacted] and [redacted] change control, but lack detailed guidance for the roles and responsibilities executed by [redacted] personnel and do not address emergency changes. Additionally, [redacted] is not consistently retaining documentation to support the change control and emergency change control process.	TSA should monitor [redacted] completion of the following: 1. Continue to develop and implement a more detailed change control policy and procedure to formally define the change control process for [redacted], [redacted] and [redacted] to include the different roles and responsibilities that personnel within Coast Guard-[redacted] must complete. Additionally, ensure that the policies and procedures developed include the emergency change control. 2. Develop and implement policies and procedures to specifically address initial approvals of the changes proposed by the software vendor, including technical changes, testing involved, and additional testing performed by [redacted] 3. Continue to develop and implement a formalized process for the retention of documentation throughout the change control process.	X		High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-23	Coast Guard has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting Coast Guard Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of [redacted] in June of 2003. [redacted] reports that the documentation and tracking of the scripts was not developed until June of 2005 but is unable to provide a complete population of implemented scripts, to include the type, purpose and intended effect on financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on financial data.	TSA should monitor CG's completion of the following: 1. Immediately implement a single, integrated change control process over Coast Guard Financial Systems with appropriate internal controls to in include clear lines of authority to Coast Guard financial management personnel, enforced responsibilities of all participants in the process and documentation requirements 2. Continue with plans to further commence an in depth examination of the Coast Guard Financial Systems with an external independent organization trained in financial information systems, process analysis and with a demonstrated understanding of the federal accounting environment to determine the root causes and specific, detailed actions necessary to correct the conditions that caused scripts as well as manual adjustments to be implemented. Coast Guard's root cause analysis needs to specifically determine if the causes are process or system driven to determine the appropriate corrective actions. 3. In conjunction with item number two above, begin an in depth examination to determine and document, in detail, the effects of the identified root causes and implemented automated and manual adjustments on financial data and affected financial statements for prior reporting periods and make appropriate restatements, if necessary.	X		High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-24	Civilian background investigations and reinvestigations are not being performed in accordance with DHS guidance. Specifically, sixteen (16) out of twenty (20) individual background investigations reviewed did not meet the DHS minimum standard of investigation of an Minimum Background Investigation (MBI) per DHS 4300A. Additionally, upon review of a selection of five (5) civilian personnel, one (1) individual had an investigation that had not been adjudicated since 1988. DHS guidance requires that civilian personnel are reinvestigated every ten (10) years.	TSA should monitor CG's completion of performing initial background investigations and reinvestigations for civilian employees in accordance with DHS directives.	X		Medium
TSA-IT-07-25	TSA has not documented policies and procedures surrounding the change control process for [redacted], formalized a tracking process of its own change requests submitted to [redacted], or retained documentation associated with the requests (i.e., initial approvals, testing and final approvals). Additionally, KPMG noted that testing was not fully completed by TSA prior to passing the change for testing for three of the changes.	TSA should complete the following: 1. Develop and implement a more detailed change control policy and procedure to formally define the change control process for [redacted] This documentation should detail the different roles and responsibilities that personnel within TSA Property Division must complete. 2. Develop and implement policies and procedures to specifically address initial approvals of the changes proposed by the software vendor, including technical changes, testing involved, and additional testing performed by [redacted]. 3. Develop and implement a formalized process for the retention of documentation throughout the change control process for [redacted]. 4. Ensure that the policies and procedures developed include the emergency change control process for [redacted]. 5: Ensure that all changes are fully tested and have passed prior to approving the change.		X	High

Exhibit D

STATUS OF PRIOR YEAR TSA IT NOTICES OF FINDING AND RECOMMENDATION

NFR No.	Description	Disposition	
		Closed	Repeat
TSA-IT 06-001	Service continuity weaknesses for [redacted], including outdated Business Continuity Contingency Plan (BCCP), lack of disaster recovery procedure details, an off-site storage location in close proximity to the data center, and lack of BCCP testing exist.		TSA-IT-07-01
TSA-IT-06-002	A comprehensive incident capability that includes designated response team members and procedures for incident handling to help ensure that the incident is properly handed has not been documented and implemented.	X	
TSA-IT-06-003	[redacted] emergency procedures are in place for the evacuation of [redacted] and its data center; however, no emergency re-entry procedures exist within this directive. Additionally, no policies and procedures are in place to guide and document the emergency training of data center personnel. Lastly, the concept of "least privilege" has not been implemented with regard to the data center.		TSA-IT-07-04
TSA-IT-06-004	Although backup tapes for [redacted] are created on a regular basis, testing procedures have not been documented in accordance with [redacted] Instruction. Additionally, although [redacted] backup tapes are rotated off-site to the [redacted], [redacted] backups have not been included in the rotation process. Lastly, tape transfer logs are not being completed in their entirety.	X	
TSA-IT-06-005	Configuration weaknesses over [redacted] workstations allowed users to modify sensitive workstation system and security settings. Upon notification, [redacted] management took immediate action to correct the configuration settings.	X	
TSA-IT-06-006	Weaknesses were noted regarding [redacted] personnel entrance and exit procedures for civilian, contractor and military personnel.	X	
TSA-IT-06-007	A [redacted] Security Configuration Management Plan does not exist that clearly delineates the roles and responsibilities between Global Computer Enterprises (GCE), and the [redacted]N. GCE is the organization under contract by Coast Guard to manage the [redacted] and [redacted] software programs. Consequently, the System Security Plans for the [redacted] and [redacted] applications do not include key security control information such as the current security configuration management process, including delineation of responsibilities for all involved parties.	X	
TSA-IT-06-008	Technical testing identified patch management weaknesses on hosts supporting the [redacted] and [redacted] applications which could allow for a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] and [redacted] data.		TSA-IT-07-18
TSA-IT-06-009	Technical testing identified configuration management weaknesses on hosts supporting the [redacted] and [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.		TSA-IT-07-19
TSA-IT-06-010	Not Used.		

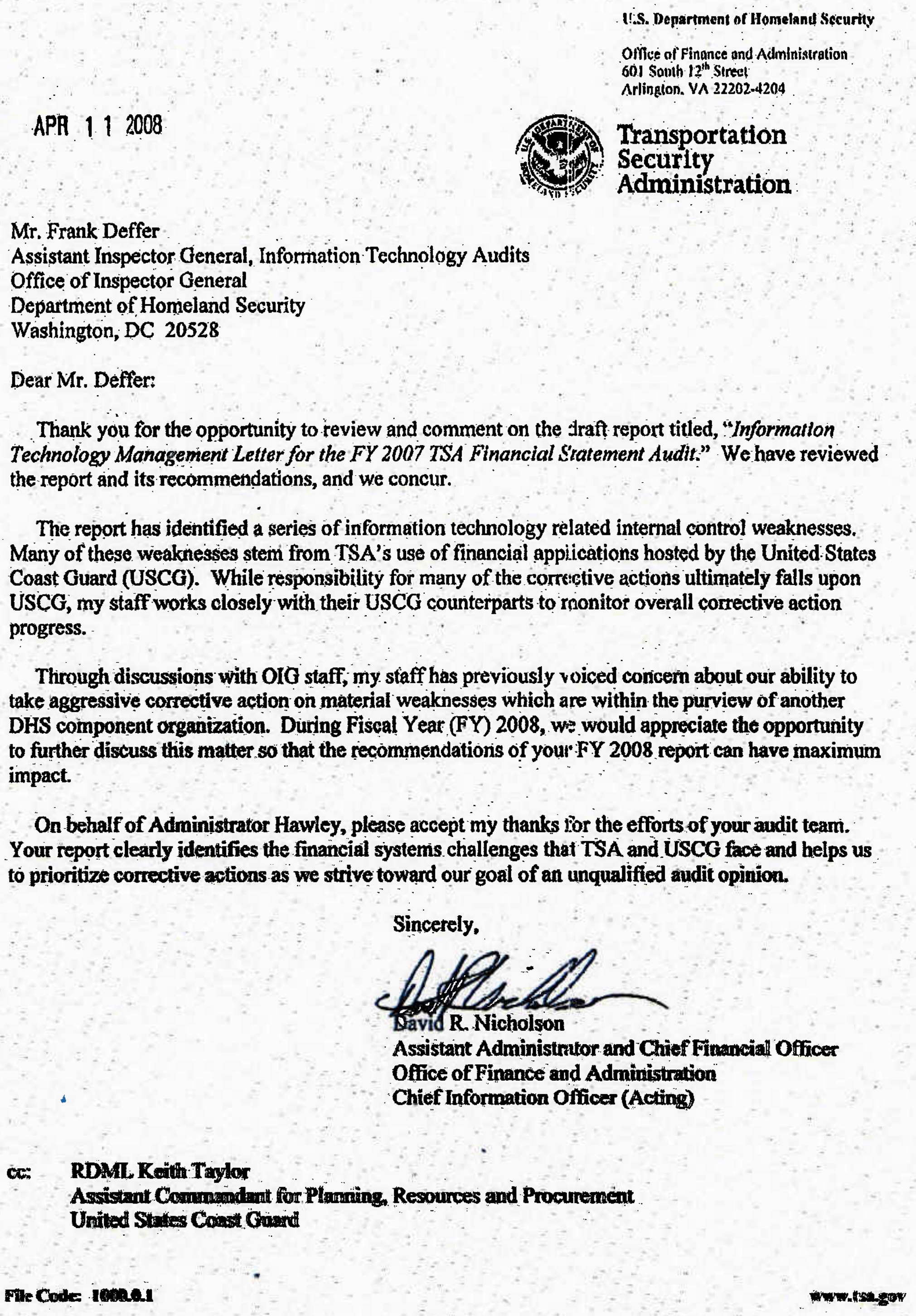
Exhibit D

NFR No.	Description	Disposition	
		Closed	Repeat
TSA-IT-06-011	The MOU between [redacted] and Treasury Financial Management Service expired during FY 2006.	X	
TSA-IT-06-012	An agreement for system software and hardware support for the four production databases including the [redacted] production database expired on May 31, 2006. A request to renew the contract is pending; however, there is no other contractual agreement to cover the maintenance of their software and hardware during this lapse in service contracts.	X	
TSA-IT-06-013	Manager Review of System Administration Monitor Procedures do not note the periods of review that are being monitored and who is responsible for performing the reviews, and evidence that the manager review was performed could only be obtained for March 2006. Additionally, for the first half of the fiscal year, Unix system administration monitoring was not performed by a manager or group outside of the three systems administrators. Additionally, [redacted] access request forms are not consistently maintained and the account of a contractor that left [redacted] remained active for eight months after the contractor's departure.	X	
TSA-IT-06-014	The following [redacted] access control weaknesses were identified: 1. Password configurations for the application and database were not in compliance with the [redacted] Password Policy Standard Operating Procedure (SOP). 2. Users are not locked out of their [redacted] application accounts after three invalid logon attempts. 3. Audit logging has not been enabled within the [redacted] application or database. 4. Individuals who were no longer employed with [redacted] were found to have active accounts within [redacted]. 5. [redacted] account reviews have not been performed on a periodic basis for [redacted] personnel.		TSA-IT-07-08
TSA-IT-06-015	The following [redacted] access control weaknesses were identified: 1. Password configurations for the application and database were not in compliance with the [redacted] Password Policy SOP. 2. Users are not locked out of their [redacted] accounts after three invalid logon attempts. 3. Policies and procedures for application and database audit log management have not been documented, and audit logs that are generated are being reviewed by the database administrators, not by an external party.		TSA-IT-07-09

Exhibit D

NFR No.	Description	Disposition	
		Closed	Closed
TSA-IT-06-016	The following [redacted] access control weaknesses were identified: 1. Password configurations for the application and database were not in compliance with the [redacted] Password Policy SOP. 2. Users are not locked out of the [redacted] application after three invalid logon attempts. 3. Audit logging has not been enabled within the [redacted] application or database.	X	
TSA-IT-06-017	[redacted] accounts are not immediately disabled upon an employee's termination, and no policies and procedures exist for the periodic review of TSA personnel with access to [redacted].		TSA-IT-07-12
TSA-IT-06-018	[redacted] accounts are not immediately disabled upon an employee's termination. Additionally, formalized policies and procedures for the periodic review of the [redacted] accounts do not exist. Lastly, [redacted] access request forms are not consistently completed.		TSA-IT-07-11
TSA-IT-06-019	[redacted] accounts are not immediately disabled upon an employee's termination. Additionally, policies and procedures do not exist requiring the periodic review of TSA personnel with access to [redacted].		TSA-IT-07-07
TSA-IT-06-020	The TSA Form 1402, IT off-boarding form for Non-Screeners and Contractors, is not consistently completed for terminated personnel. Specifically, we identified that the form was unavailable for thirty-eight (38) of sixty (60) terminated employees selected for testing. Additionally, eight (8) out of the twenty-two (22) forms received were incomplete.		TSA-IT-07-20
TSA-IT-06-021	Security awareness training and Computer Access Agreements are not consistently completed. Additionally, TSA has not documented sanctioning procedures to be enforced when users of TSA information systems are in violation of the computer access agreements and security policies.		TSA-IT-07-15
TSA-IT-06-022	TSA has not documented policies and procedures surrounding the change control process for [redacted], formalized a tracking process of its own change requests submitted to [redacted], or retained documentation associated with the requests (i.e., initial approvals, testing and final approvals).		TSA-IT-07-21 and TSA-IT-07-25
TSA-IT-06-023	Guidance for performing suitability screening for all contractors is considered interim and not final; therefore, Coast Guard will wait until the policy is finalized before moving forward on conducting background investigations on contractors. Additionally, [redacted] does not perform background investigations or verify that outside background investigations have been performed for contractors working at [redacted]. Lastly, risk levels for contractor personnel with access to DHS information systems have not been assigned.		TSA-IT-07-05
TSA-IT-06-024	Excessive access has been granted within [redacted]. Specifically, of the 27 individuals that have been granted Authorized Certifying Officer privileges to approve invoices of any dollar value, four were not justified in having such privileged access.	X	

Exhibit E



U.S. Department of Homeland Security

Office of Finance and Administration
601 South 12th Street
Arlington, VA 22202-4204

APR 11 2008

Transportation
Security
Administration

Mr. Frank Deffer
Assistant Inspector General, Information Technology Audits
Office of Inspector General
Department of Homeland Security
Washington, DC 20528

Dear Mr. Deffer:

Thank you for the opportunity to review and comment on the draft report titled, "*Information Technology Management Letter for the FY 2007 TSA Financial Statement Audit*." We have reviewed the report and its recommendations, and we concur.

The report has identified a series of information technology related internal control weaknesses. Many of these weaknesses stem from TSA's use of financial applications hosted by the United States Coast Guard (USCG). While responsibility for many of the corrective actions ultimately falls upon USCG, my staff works closely with their USCG counterparts to monitor overall corrective action progress.

Through discussions with OIG staff, my staff has previously voiced concern about our ability to take aggressive corrective action on material weaknesses which are within the purview of another DHS component organization. During Fiscal Year (FY) 2008, we would appreciate the opportunity to further discuss this matter so that the recommendations of your FY 2008 report can have maximum impact.

On behalf of Administrator Hawley, please accept my thanks for the efforts of your audit team. Your report clearly identifies the financial systems challenges that TSA and USCG face and helps us to prioritize corrective actions as we strive toward our goal of an unqualified audit opinion.

Sincerely,

David R. Nicholson
Assistant Administrator and Chief Financial Officer
Office of Finance and Administration
Chief Information Officer (Acting)

cc: RDML Keith Taylor
Assistant Commandant for Planning, Resources and Procurement
United States Coast Guard

File Code: 1000.0.1

www.tsa.gov

Transportation Security Administration
Information Technology Management Letter
For the FY 2007 TSA Balance Sheet Audit

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Acting Assistant Commissioner, TSA
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, TSA
Chief Information Officer, TSA
Chief Information Security Officer
Assistant Secretary for Policy
Assistant Secretary for 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, call the Office of Inspector General (OIG) at (202) 254-4199, 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.