DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Special Report: Letter on Information Technology Matters Related to TSA's FY 2005 Financial Statements (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552 (b)(2). A review under the Freedom of Information Act will be conducted upon request.

OIG-07-18 **December 2006**

Office of Inspector General

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

Homeland Security

December 8, 2006

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 published by our office as part of our DHS oversight responsibility to promote economy, efficiency, and effectiveness within the department.

This special report presents a letter on information technology (IT) matters related to TSA's FY 2005 financial statements prepared by the independent public accounting firm KPMG LLP (KPMG). We engaged KPMG to audit TSA's FY 2005 financial statements. KPMG did not complete their audit because TSA did not provide KPMG with final financial statements on which KPMG could report.

The recommendations herein have been discussed in with those responsible for implementation. It is our hope that this report with KPMG's attached letter 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

March 14, 2006

Mr. Richard L. Skinner
Inspector General
U.S. Department of Homeland Security
245 Murray Drive, S.W. Bldg. 410
Washington D.C. 20528

Dear Mr. Skinner:

We were engaged to audit the consolidated balance sheet of the U.S. Department of Homeland Security's Transportation Security Administration (TSA) as of September 30, 2005, and the related consolidated statements of net cost, changes in net position, and financing, and the combined statement of budgetary resources, for the year then ended (hereinafter referred to as the consolidated financial statements). TSA's management is responsible for preparing its consolidated financial statements.

We did not audit, review, or complete procedures related to the consolidated financial statements because management did not present final consolidated financial statements for audit. Accordingly, we are unable to provide an auditors' report on the consolidated financial statements.

In connection with our engagement to audit the consolidated financial statements, we were also engaged to consider TSA's internal control over financial reporting and to test 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 financial statements. Our procedures do not include examining the effectiveness of internal control and do not provide assurance on internal control.

However, we noted certain matters involving internal control and other operational matters with respect to information technology that are summarized and presented in Attachment A for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve information technology internal control or result in other operating efficiencies. Attachments B – D present additional information for management's use. Attachment E presents management's response to the draft of this letter. We have separately communicated to you certain matters involving internal control and other operational matters noted that do not relate to information technology. Further, other matters involving internal control over information technology may have been identified had we been able to perform all procedures necessary to express an opinion on the consolidated financial statements. We would be pleased to discuss these comments and recommendations with you at any time.

Very truly yours,

KPMG LLP

SUMMARY OF FINDINGS AND RECOMMENDATIONS

The U.S. Coast Guard's ---------- hosts key financial applications for the U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA). As such, our audit procedures over IT general controls for TSA included a review of the Coast Guard's ---------- procedures, policies, and practices. While we noted that ---------- took corrective actions to address prior year IT control weaknesses that impact the TSA financial processing environment, we continued to find IT general control weaknesses. Collectively, the IT control weaknesses limited TSA's ability to ensure that critical financial and operational data was maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over TSA financial reporting and its operation.

We noted that many of the conditions identified during our prior year audits, which impact TSA financial processing, have not been corrected because challenges continue to exist related to the merging of numerous IT functions, controls, processes, and overall organizational shortages. During FY 2005, the Coast Guard ---------- took steps to help address known weaknesses, such as conducting periodic vulnerability assessments of security controls, increasing controls over access to sensitive application functions, and implementing practices that adhere to guidance issued in the update to DHS Policy 4300A, *Sensitive System Handbook.*

Despite these improvements, TSA and Coast Guard management should ensure that there is emphasis on the monitoring and enforcement of IT security-related policies and procedures. On-going measures to certify and accredit key financial systems hosted by -- -------- and implement effective disaster recovery and continuity of operations 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 instituting a formal process for performing scans of the ------ ---- network environment to ensure that security settings, once instituted, remain in place and to identify vulnerabilities that require correction.

IT GENERAL CONTROL FINDINGS BY AREA

Entity-Wide Security Program Planning and Management

During FY 2005, we noted that the Coast Guard -- -------- had made progress towards improving entity-wide security program planning and management. However, the Coast Guard ------ ---- has not completed Certification and Accreditation (C&A) efforts for the ---------- ----- ---------- ---------- ----- ---------- ---------- ---- ----------
Particularly, security testing and evaluation was incomplete and security plans had not been updated.

Recommendation:

Entity-wide security program planning and management controls should be in place to establish a framework and continuing cycle of activity to manage security risk, develop security policies, assign responsibilities, and monitor the adequacy of computer security related controls. We recommend that the TSA Chief Financial Officer (CFO) and Chief Information Officer (CIO) offices work with ---------- management and the Coast Guard CIO, to ensure that the C&A process for key financial systems affecting TSA processing is completed, including the completion of security tests and evaluations and the update of security plans.

Access Controls

In close concert with an organization's entity-wide information security program, 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.

During FY 2005, we noted that the Coast Guard ---------- began conducting periodic vulnerability assessments to identify system and network security risks. While this resulted in a reduced number of identified vulnerabilities, we did note several repeat access control weaknesses, including some related to access control vulnerabilities with ---------- ---------- ---------- --. 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 some systems and applications. Some of the identified vulnerable devices are used for ---- and ---------- purposes. In some cases, users are able to access test and development devices with group passwords, system default passwords, or the same passwords with which they log into ---------- --- As a result, ---------- ---------- --- ---------- could be a target of hackers/crackers to obtain information (i.e., ---------- ------ --------) that can be used to attempt further access into the DHS IT environment.

Conditions noted at the Coast Guard ---------- regarding access controls that impact TSA's financial processing are as follows:

- Instances of missing and weak user passwords on ---- ---------- were identified.
- Instances were identified where workstations, servers, or network devices were configured without necessary security patches, or were not configured in the most secure manner.
- Policies and procedures requiring local security administrators to periodically revalidate ----- user profiles were not implemented. Additionally, evidence of reviews of ----- for the removal of accounts for separated personnel was not available.
- High-level ------database administrator, system administrator, and system accounts were not actively monitored.
- Procedures for the authorization, regular review, and removal of data center physical access were not formalized and were inconsistent.
- Information system-related items (e.g., hardware, software, and electronic media) entering and exiting the -- -------- facility were not adequately tracked or recorded.

Recommendation:

We recommend that the TSA CFO and CIO offices work with ---------- management and the Coast Guard CIO, to ensure the following corrective actions are implemented:

- Enforce password controls that meet DHS password requirements, as prescribed in DHS Policy 4300A, *Sensitive System Handbook*, on all key financial systems.

- Implement a formal process for performing periodic scans of the - ----------network environment, including the financial processing environment, for the identification and correction of vulnerabilities, in accordance with DHS 4300A DHS Policy and Federal guidance, the National Institute of Standard and Technology, Special Publication, 800-42, Guideline on Network Security Testing.

- Develop formal entity-wide procedures for controlling the processes associated with the granting, monitoring, and terminating of ----- user accounts that require the periodic revalidation of ----- user profiles by local security administrators.

- Develop procedures for the regular and periodic monitoring of high-level ----- database administrators, system administrators, and system accounts to ensure that transactions are authorized and appropriate. The reviews should be performed by an individual in management that does not have the same logical access authority.

- Develop and implement formal -- -------- data center access procedures for requesting, granting, and removing access to the data center; performing regular reviews of physical access privileges; and retaining evidence of such reviews.

- Develop, document, and implement a formalized method to track information system-related items entering and exiting the ---------- facility and maintain appropriate records.

Application Software Development and Change Control

During FY 2005, we noted that the Coast Guard's ---------- took corrective actions to address IT control issues related to application software changes. However, we noted that in some cases the application software development and change control procedures and documentation were not consistent with DHS and Federal guidance. Regarding application software development and change controls that impact TSA's financial processing, we noted instances of weakness in change control processes supporting the ---------- - ----- - Specifically, procedures were not developed, documentation supporting risk assessments of software patches was not retained, formal change request forms were not in use, and test plans and results were not documented.

Recommendation:

We recommend that the TSA CFO and CIO offices work with ---------- management and the Coast Guard CIO, to ensure that the following corrective actions are implemented:

- Develop and enforce configuration management procedures for development of test plans, documentation of test results, delivery and implementation of software, and management approval of system changes for normal and emergency upgrade situations.

- Retain all risk assessment and testing documentation to provide an audit trail for all changes.

System Software

We noted weaknesses in programs designed to operate and control the processing activities of computer equipment. Weaknesses in this control area, closely linked to entity-wide security and access controls, increase the likelihood that unauthorized individuals using system software could circumvent security controls to read, modify, or delete critical or sensitive information and programs. Authorized users of the system could gain unauthorized privileges to conduct unauthorized actions, and/or systems software could be used to circumvent edits and other controls built into application programs.

Regarding system software controls at the Coast Guard ---------- that impact TSA's financial processing, we noted that policies and procedures for restricting and monitoring access to operating system software were not developed or were inadequate.

Recommendation:

We recommend that the TSA CFO and CIO offices work with ---------- management and the Coast Guard CIO, to ensure that the following corrective actions are implemented:

- Develop policies and procedures to address access to ----- and ----- in the operating system environment that include steps for granting, approving, and reviewing access; definitions of levels of access; and steps for terminating access for ----- and -----.

- Develop policies and procedures for the type of monitoring that each ------- system administrator should perform both on a daily and periodic basis, and periodically test the effectiveness of the current monitoring process to ensure that unauthorized events are correctly identified.

Service Continuity

During FY 2005, we noted that the Coast Guard had begun corrective actions to address prior year weaknesses related to the back-up and protection of critical system data. Despite these improvements, weaknesses related to disaster recovery plans and business continuity plans continue to exist. These issues are important because losing the capability to process, retrieve, and protect information maintained electronically can significantly affect TSA's ability to accomplish its mission.

Conditions noted at the Coast Guard - --------- regarding service continuity controls that impact TSA's financial processing are as follows:

- The ---------- business continuity plan did not adequately include procedures for restoring ----- and ----- financial systems, and disaster recovery plans for the systems had not been developed.
- Relocation of the off-site storage location to a geographically safe distance from the primary data center was not complete.
- The -------- -- business continuity plan had not been tested or updated to reflect changes in hardware, software, or the off-site storage location.

Recommendation:

We recommend that the TSA CFO and CIO offices work with ---------- management and the Coast Guard CIO, to ensure that the following corrective actions are implemented:

- Periodically reassess and, as appropriate, revise the ---------- business continuity plan to reflect changes in hardware, software, and the off-site storage location, and include adequate steps for the restoration of financial systems.

- Develop disaster recovery procedures for ----- and ----- that detail processes for re-establishing hardware, software, and telecommunications connectivity.

- Complete the relocation of the off-site storage location further away from the -- -------- primary data center.

- Periodically test the business continuity plan and evaluate the results so that the plan can be adjusted to correct any deficiencies identified during testing.

APPLICATION CONTROL FINDINGS

During FY 2005, we noted weaknesses in access and account management controls associated with key TSA financial applications hosted by -- --------, such as the core financial and procurement applications. Many of these weaknesses were identified during our general controls testing; however, since these same issues also impact controls over specific key financial applications, they are reported here as well.

Conditions noted regarding application controls that impact TSA's financial processing are as follows:

- Instances of missing and weak user passwords on key application servers and databases were identified.

- Policies and procedures requiring local security administrators to periodically revalidate ----- user profiles were not implemented. Additionally, evidence of reviews of ----- user accounts for the removal of accounts for separated personnel was not available.

- High-level ----- database administrator, system administrator, and system accounts were not actively monitored.

- Certain erroneous personnel records had not been corrected.

Recommendation:

We recommend that the TSA CFO and CIO offices work with ----------management and the Coast Guard CIO, to ensure that the following corrective actions are implemented:

- Enforce password controls that meet DHS password requirements, as prescribed in DHS Policy 4300A, *Sensitive System Handbook,* on all key financial systems.

- Develop formal entity-wide procedures for controlling the processes associated with the granting, monitoring, and terminating of ----- user accounts that require the periodic revalidation of ----- user profiles by local security administrators.

- Develop procedures for the regular and periodic monitoring of high-level ----- database administrators, system administrators, and system accounts to ensure that transactions are authorized and appropriate. The reviews should be performed by an individual in management that does not have the same logical access authority.

- Ensure that erroneous personnel records are corrected and that evidence of corrective actions taken is retained on file.

MANAGEMENT COMMENTS AND OIG EVALUATION

We obtained written comments on a draft of this report from the TSA Assistant Administrator for Finance and Administration and Chief Financial Officer. Generally, the TSA CFO agreed with all of the report's findings and recommendations. We have incorporated the comments where appropriate and included a copy of the comments in their entirety at Appendix E.

In his response, the TSA CFO stated that:

- The report identified a series of information technology related internal control weaknesses that stem from TSA's use of the United States Coast Guard (USCG) financial application.
- During FY 2006, the USCG began corrective actions on these weaknesses.
- TSA will continue to work closely with the USCG in FY 2007 to address the outstanding FY 2005 findings.

OIG Response

We agree with the steps that TSA and USCG are taking to satisfy these recommendations.

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE

Below is a description of significant TSA financial management systems and supporting IT infrastructure included in the scope of the FY 2005 financial statement audit engagement.

Locations of Testing:
---------- ---------- -------- ---------- --- ---------- TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Testing:
The Coast Guard is TSA's accounting services provider. The following is a list of key TSA applications used for financial processing.

- ---------- ---------- is the core accounting system that records financial transactions and generates financial statements for TSA. ----- is hosted at ----------, the Coast Guard's primary data center.

- ---------- ---------- ---------- application is used to create and post obligations to -----. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly -- ------- ------ ---------- Reports.

- -- - ---------- --- -is the document image processing system, which is integrated with an ------ ---------- ------ relational database. -- ---- allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation, and payment. ------- utilizes MarkView software to scan documents, to view the images of scanned documents, and to render images of electronic data received.

- ---------- ---------- ------- maintains TSA payroll data; calculates pay, wages, and tax information; and maintains service history and separation records. ----- - - interfaces with the -------- ---------- - ------- ----- ------- ----------, and the ---------- - ------- ---------- ---------, and receives other data inputs. ------- is a mainframe application.

- ---------- ---------- ---------- --- – --------- is the U.S. Department of Transportation's (DOT) personnel management system. The system processes and tracks personnel actions and employee related data for TSA, including employee elections for the Thrift Savings Plan (TSP), life insurance, and health insurance as well as training data and general employee information (e.g., name and address). --- ----- is also used to maintain information related to budget, training, civil rights, labor relations and security. --------- is a mainframe application. --------- interfaces with --------to allow ------- to perform the calculation of pay, time and attendance reporting, leave accounting, and wage and tax reporting. ------- also uses the

information received from [redacted] to initiate payroll deductions for TSP, insurances, Combined Federal Campaign contributions, and savings bonds.

- [redacted] – [redacted] processes requests for personnel action, training enrollments, and time and attendance information. [redacted] interfaces with [redacted] and [redacted] to receive time and attendance and payroll information. [redacted] also interfaces with the [redacted] system. [redacted] is a client/server system that provides reporting capability through an Oracle database.

On August 22, 2005, TSA payroll and time and attendance processing moved to the National Finance Center (NFC) system administered by the Department of Agriculture. For payroll, TSA will be using [redacted], which will interface with the NFC system. The [redacted]. The [redacted] system will also interface with the NFC system.

TSA IT NOTICES OF FINDINGS AND RECOMMENDATIONS THAT CONTRIBUTED TO THE DEPARTMENT'S MATERIAL WEAKNESS OVER FINANCIAL SYSTEM SECURITY

NFR #	Condition	Recommendation	New Issue	Repeat Issue
TSA-IT 05-001	Formal procedures regarding access to the [redacted] data center have not been established and implemented.	TSA management should work with [redacted] management to ensure the development and implementation of formal data center access procedures and a formalized method to track information system-related items entering and exiting the facility.	**X**	
TSA-IT 05-002	Was not used.	N/A	N/A	N/A
TSA-IT-05-003	[redacted] change control process supporting [redacted] and [redacted] have weaknesses including: procedures in support of the finalized CM policy are not developed, documentation supporting a risk assessment is not maintained, formal change requests are not used, and test plans and test results are not documented.	TSA management should work with [redacted] management to ensure the development and enforcement of configuration management procedures for developing test plans, documenting test results, implementing software, management approval of system changes, and retention of risk assessment and testing documentation.	**X**	
TSA-IT-05-004	Service continuity weaknesses for [redacted], [redacted], and [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 management should work with [redacted] management to ensure the periodic reassessment and, as appropriate, revision of the [redacted] BCCP, development of disaster recovery procedures for [redacted] and [redacted], completion of the relocation of the off-site storage location, and periodic testing of the BCCP.	**X**	

NFR #	Condition	Recommendation	New Issue	Repeat Issue
TSA-IT-05-005	Documented procedures do not exist for controlling the processes associated with the granting, monitoring, and termination of user accounts within -----.	TSA management should work with - --------- management to ensure the development of formal entity wide procedures for granting, monitoring, and terminating ----- user accounts and periodic revalidation of ----- user profiles by local security administrators.	**X**	
TSA-IT 05-006	-------- -- has not developed documented policies and procedures to restrict access to the ------- operating system, to monitor access to this system, and for periodic reviews to determine if monitoring of the ------ operating system for ------ and ----- is functioning as intended.	TSA management should work with - --------- management to ensure the development of policies and procedures for restricting and monitoring access to the ------- operating system for ----- and - - -- and performance of period reviews of the monitoring process.	**X**	
TSA-IT 05-007	Certification and Accreditation (C&A) of the ----- -- --- ---------- ---------- ----- ----- --- -- ----- ---- - -----, and ----- was not complete. Specifically, security testing and evaluation (ST&E) was incomplete and security plans had not been updated.	TSA management should work with - --------- management to ensure the update and completion of the C&A process for --- ---- ------, and ----- to include the completion of ST&E, and the update of security plans.	**X**	
TSA-IT-05-008	-------- -- has not implemented formal procedures for the periodic management review and monitoring of activities of ----- database administrators, system administrators, and the -------- SYS accounts.	TSA management should work with - --------- management to ensure the development of procedures for the regular and periodic monitoring of high-level ----- database administrator and system administrator activities, and the -------- SYS account.	**X**	

NFR #	Condition	Recommendation	New Issue	Repeat Issue
TSA-IT-05-009	The Enterprise Security Management tool identified world writeable directories without a sticky bit set and account management weaknesses over ------- .	TSA management should work with - --------- management to ensure the implementation of the individual fixes noted in the NFR for vulnerabilities identified and the institution of a formal process for performing periodic scans of the -- ----- -- network environment, including the financial processing environment.	**X**	
TSA-IT-05-010	AppDetective identified vulnerabilities on the ----- database including weak passwords, excessive access permissions and missing patches.	TSA management should work with - --------- management to ensure the implementation of the individual fixes noted in the NFR for vulnerabilities identified and institution of a formal process for performing periodic scans of the -- ----- -- network environment, including the financial processing environment.	**X**	
TSA-IT-05-011	Internet Security Systems Internet Scanner identified three hosts that were missing patches.	------ - -- management implemented immediate corrective action by removing the --- --- -- -- ------ from the three hosts.	**X**	
TSA-IT 05-012	Inaccuracies exist within TSA personnel records which address separated employee issues and other erroneous personnel records.	TSA management should ensure that personnel errors regarding separated employees cited during the prior year audit are corrected and documentation of corrective actions is retained on file.		**X**

STATUS OF PRIOR YEAR TSA IT NOTICES OF FINDINGS AND RECOMMENDATIONS

NFR No.	Description	Disposition	
		Closed	Repeat
04-01	Segregation of duties is not properly enforced in the Delphi Application within FFMS.	**X**	
04-02	Weaknesses in Delphi access controls, network security, and system security controls.	**X**	
04-03	System financial integrity issues identified in the Delphi application.	**X**	
04-04	Inaccuracies exist within TSA personnel records which addresses both separated employee issue and other erroneous personnel records.		05-012

U.S. Department of Homeland Security
Arlington, VA 22202-4204

Transportation
Security
Administration

NOV 17 2006

Mr. Frank Deffer
Assistant General Inspector, 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, "Letter on Information Technology Matters Related to TSA's FY 2005 Financial Statements." We have reviewed the report and its recommendations, and we concurred with the report under separate cover.

The report has identified a series of information technology related internal control weaknesses, which stem from TSA's use of the United States Coast Guard (USCG) financial applications. These weaknesses may limit TSA's ability to ensure that financial and operational data is maintained in accordance with applicable information security standards. Accordingly, we request that certain portions of the report which describe the nature of the security weaknesses be excluded from public release. Specifically, we would request that following content be excluded:

- Attachment A, content under the heading "IT General Control Findings by Area.
- Attachment A, content under the heading "Application Control Findings."
- Attachment C, in its entirety.

These portions of the report describe specific system security weaknesses in detail. As stated in our response, USCG has resolved several of the weaknesses and is taking action to resolve those that remain open. Public release of data on our vulnerabilities is potentially harmful and not in the best interest of TSA, USCG, or DHS.

We appreciate your consideration of this request.

Sincerely,

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

cc: RDML Robert S. Branham
Assistant Commandant for Planning, Resources and Procurement
United States Coast Guard

www.tsa.gov

U.S. Department of Homeland Security
Arlington, VA 22202-4204

Transportation
Security
Administration

NOV -7 2006

Mr. Frank Deffer
Assistant General Inspector, 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 "Letter on Information Technology Matters Related to TSA's FY 2005 Financial Statements." We have reviewed the report and its recommendations, and we concur with the report.

The report has identified a series of information technology related internal control weaknesses. These weaknesses stem from TSA's use of the United States Coast Guard (USCG) [redacted] While corrective actions are ultimately implemented by USCG, my staff works closely with USCG [redacted] to analyze underlying problems, clarify system requirements, and monitor overall progress.

During FY 2006, USCG began corrective action on these weaknesses. Of the eleven findings noted in Attachment C of the draft report, seven have been closed by KPMG as part of the FY 2006 financial statement audit and corrective action is ongoing for the remaining four. The enclosure provides status of corrective action for each specific finding presented in the draft report.

TSA will continue to work closely with USCG in FY 2007 to address the outstanding FY 2005 findings and additional conditions identified during the FY 2006 financial statement audit.

If you have additional questions or wish to discuss the ongoing corrective actions, please contact Mr. David Lanagan, Chief, Internal Control Branch, at (571) 227-3091.

Please note that our comments regarding public release of the report are being provided under separate cover.

Sincerely,

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

Enclosure

cc RDML Robert S. Branham
Assistant Commandant for Planning, Resources and Procurement
United States Coast Guard

TSA FY 2005 Financial Statement Audit
Information Technology Related Notices of Findings & Recommendations (NFR)
Status as of October 2006

NFR #	Condition	Recommendation	Status
TSA-IT-05-001	Formal procedures regarding access to the data center have not been established and implemented.	TSA management should work with management to ensure the development and implementation of formal data center access procedures and a formalized method to track information system-relates items entering and exiting the facility.	Closed by KPMG during FY 2006 financial statement audit.
TSA-IT-05-003	change control process supporting and have weaknesses including: procedures in support of the finalized CM policy are not developed, documentation supporting a risk assessment is not maintained, formal change requests are not used, and test plans and test results are not documented.	TSA management should work with management to ensure the development and enforcement of configuration management procedures for developing test plans, documenting test results, implementing software, management approval of system changes, and retention of risk assessment and testing documentation.	Closed by KPMG during FY 2006 financial statement audit.
TSA-IT-05-004	Service continuity weaknesses for 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 management should work with management to ensure the periodic reassessment and, as appropriate, revision of the BCCP, development of disaster recovery procedures for and completion of the relocation of the off-site storage location, and periodic testing of the BCCP.	Resolution ongoing.
TSA-IT-05-005	Documented procedures do not exist for controlling the processes associated with the granting, monitoring, and termination of user accounts within	TSA management should work with management to ensure the development of formal entity wide procedures for granting, monitoring, and terminating user accounts and periodic revalidation of user profiles by local security administrators.	Closed by KPMG during FY 2006 financial statement audit.
TSA-IT-05-006	has not developed documented policies and procedures to restrict access to the operating system, to monitor access to this system, and for periodic reviews to determine if monitoring of the operating system for is functioning as intended.	TSA management should work with management to ensure the development of policies and procedures for restricting and monitoring access to the operating system for and performance of periodic reviews of the monitoring process.	Resolution ongoing.

TSA FY 2005 Financial Statement Audit
Information Technology Related Notices of Findings & Recommendations (NFR)
Status as of October 2006

NFR #	Condition	Recommendation	Status
TSA-IT-05-007	Certification and Accreditation (C&A) of the [redacted] and [redacted] was not complete. Specifically, security testing and evaluation (ST&E) was incomplete and security plans had not been updated.	TSA management should work with [redacted] management to ensure the update and completion of the C&A process for [redacted], and [redacted] to include the completion of ST&E, and the update of security plans.	Closed by KPMG during FY 2006 financial statement audit.
TSA-IT-05-008	[redacted] has not implemented formal procedures for the periodic management review and monitoring of activities of [redacted] database administrators, system administrators, and the [redacted] SYS accounts.	TSA management should work with [redacted] management to ensure the development of procedures for the regular and periodic monitoring of high-level [redacted] database administrator and system administrator activities, and the [redacted] SYS account.	Closed by KPMG during FY 2006 financial statement audit.
TSA-IT-05-009	The Enterprise Security Management tool identified world writeable directories without a sticky bit set and account management weakness over DART.	TSA management should work with [redacted] management to ensure the implementation of the individual fixes noted in the NFR for vulnerabilities identified and the institution of a formal process for performing periodic scans of the [redacted] network environment, including the financial processing environment.	Resolution ongoing.
TSA-IT-05-010	AppDetective identified vulnerabilities on the [redacted] database including weak passwords, excessive access permissions and missing patches.	TSA management should work with [redacted] management to ensure the implementation of the individual fixes noted in the NFR for vulnerabilities identified and the institution of a formal process for performing periodic scans of the [redacted] network environment, including the financial processing environment.	Resolution ongoing.
TSA-IT-05-011	Internet Security Systems Internet Scanner identified three hosts that were missing patches.	[redacted] management implemented immediate corrective action by removing the BrightStor agent from the three hosts.	Closed by KPMG during FY 2006 financial statement audit.
TSA-IT-05-012	Inaccuracies exist within TSA personnel records which address separated employee issues and other erroneous personnel records.	TSA management should ensure that personnel errors regarding separated employees cited during the prior year audit are corrected and documentation of corrective actions is retained on file.	Closed by KPMG during FY 2006 financial statement audit.

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Under Secretary, Management
Director, TSA
Chief Information Officer
Deputy Chief Information Officer
Chief Financial Officer
Chief Information Officer, TSA
Chief Financial Officer, TSA
Assistant Secretary, Public Affairs
Assistant Secretary, Policy
Assistant Secretary, Legislative and Intergovernmental Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer Audit Liaison
TSA Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS Office 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) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

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 the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.