DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Information Technology Management Letter for the FY 2007 Customs Border and Protection Financial Statement Audit (Redacted)

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

OIG-08-50 May 2008

Office of Inspector General

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

Homeland Security

May 6, 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 Customs and Border Protection's (CBP) financial statement 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-08-12, November 2007) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of CBP's FY 2007 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 14, 2007, 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
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 14, 2007

Inspector General
U.S. Department of Homeland Security

Commissioner
Bureau of Customs and Border Protection

Chief Information Officer
Bureau of Customs and Border Protection

We have audited the consolidated balance sheets of the U.S. Department of Homeland Security's Bureau of Customs and Border Protection (CBP) as of September 30, 2007 and 2006, and the related consolidated statements of net cost, changes in net position, custodial activity and the combined statement of budgetary resources (hereinafter, referred to as "consolidated financial statements") for the years then ended. In planning and performing our audit of CBP's consolidated financial statements, we considered CBP's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements.

In connection with our fiscal year 2007 engagement, we considered CBP's internal control over financial reporting by obtaining an understanding of CBP's internal controls, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in Government Auditing Standards and OMB Bulletin No. 07-04, Audit Requirements for Federal Financial Statements. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA). The objective of our engagement was not to provide an opinion on the effectiveness of CBP's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of CBP's internal control over financial reporting.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects CBP's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally-accepted accounting principles such that there is more than a remote likelihood that a misstatement of CBP's financial statements that is more than inconsequential will not be prevented or detected by CBP's internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by CBP's internal controls.

During our audit, we noted certain matters involving internal control and other operational matters with respect to information technology that are summarized in the Information Technology Management Letter starting on page 1. These comments contribute to the material weakness presented in our *Independent Auditors' Report*, dated November 13, 2007, and represent the separate restricted distribution report mentioned in that report.

KPMG

The comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR); and are intended **For Official Use Only**. We aim to use our knowledge of CBP's organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report.*

The Table of Contents on the next page identifies each section of the letter. In addition, we have provided: a description of key financial systems and information technology infrastructure within the scope of the FY 2007 CBP financial statement audit is provided in Appendix A, a description of each internal control finding is provided in Appendix B, and the current status of the prior year NFRs is presented in Appendix C.

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

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

We have audited the consolidated balance sheets of the U.S. Department of Homeland Security's Bureau of Customs and Border Protection (CBP) as of September 30, 2007 and 2006, and the related consolidated statements of net cost, changes in net position, custodial activity and the combined statement of budgetary resources for the years then ended. The overall objective of our audit was to evaluate the effectiveness of IT general controls of CBP's financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office, formed the basis of our audit. The scope of the IT general controls assessment included testing at CBP's Office of Information Technology (OIT) and other offices related to the IT general controls portion of the financial statement audit.

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 (EWS)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software (SS)* – Controls that limit and monitor access to powerful programs that operate computer hardware.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Service continuity (SC)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

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

In addition to testing CBP's general control environment, we performed application control tests on a limited number of CBP 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.

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

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2007, CBP took corrective action to address prior year IT control weaknesses. For example, CBP made improvements in its certification and accreditation program, specially related to its Administrative Applications and [redacted] Also, issues with access controls related to the Systems, Applications and Products (SAP) system were addressed. However, during FY 2007, we continued to identify IT general control weaknesses at CBP. The most significant weaknesses from a financial statement audit perspective related to controls over access to programs and data and controls over program changes. Collectively, the IT control weaknesses limited CBP's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over CBP financial reporting and its operation and we consider them to collectively represent a material weakness for CBP under standards established by the American Institute of Certified Public Accountants (AICPA). The information technology findings were combined into one material weakness regarding Information Technology for the FY 2007 audit of the CBP consolidated financial statements.

Although we noted improvement, many of the conditions identified at CBP in FY 2006 have not been corrected because CBP still faces challenges related to the merging of numerous IT functions, controls, processes, and organizational resource shortages. During FY 2007, CBP took steps to address these conditions. Despite these improvements, CBP needs further emphasis on the monitoring and enforcement of access controls as well as implementing and enforcing the CBP-wide security certification and accreditation (C&A) program. Many of the issues identified during our review, which were also identified during FY 2006 and prior can be addressed through a more consistent and effective security C&A program and security training program.

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

IT GENERAL CONTROL FINDINGS BY AREA

Entity-Wide Security Program Planning and Management

During FY 2007, CBP improved its level of entity-wide security program planning and management. However, continued efforts are needed, especially in the areas of program management related to the detection and monitoring of technical information security weaknesses. As identified in prior year issues reported in FY 2003, FY 2004, FY 2005 and FY 2006, we noted that improvements are still needed in CBP's Incident Handling and Response Capability which may potentially limit CBP's ability to respond to incidents in an appropriate manner. Collectively, the identified entity-wide security planning and management issues, coupled with the access control issues described later in this management letter, reduce the overall effectiveness of the entity-wide security programs for CBP.

1 Conditions noted regarding entity-wide security program planning and management were the following:

- will not be installed on all workstations for the majority of the fiscal year.
- A complete listing of workstations is not maintained by System Security. System Security does not have the ability to quickly compile a listing of all workstations under CBP's ownership.
- The completion of security awareness training is not appropriately tracked at CBP.
- The following documents did not have proper documented approval and/or approval dates:
  - SDLC Configuration Management Plan
  - Production Management Team Procedures
- The process has several weaknesses. KPMG Consequently, KPMG was not able to determine whether the reviews of specific of roles were performed at these ports/headquarters. The is not consistently executed at the various ports. Appropriate documentation is not maintained for all recertifications.
- Virus protection is not installed on all CBP workstations.
- The did not have an Information Systems Security Officer (ISSO), but had been assigned an interim ISSO. This interim ISSO was not formally documented as the ISSO.

Recommendations:

1. We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders consider the following actions:

- should be installed on all workstations under CBP control.
- The use of local workgroups should be eliminated. All CBP workstations should be included in a CBP administered domain. Also, the CBP CIO should compile and regularly maintain a

full and accurate listing of CBP workstations and use this list to monitor and maintain patch levels for all CBP workstations.

- Security awareness training should be completed in a timely manner by all employees with access to CBP information systems. CBP should continue to work towards implementing online training for all personnel to facilitate automated tracking of the completion of security awareness training.
- Procedures should be implemented and enforced in OIT divisions to perform a review of all documentation to update, consolidate and approve the documented procedures in use by operational personnel.
- Procedures should be applied as outlined in the newly distributed memorandum from Office of Field Operations dated April 27, 2007 while consistently documenting results of recertifications at the port level and maintaining said documentation.
- Since the initial testing was performed, CBP has begun immediate remediation. CBP should continue remediation to ensure that antivirus protection is installed on all workstations under the control of CBP.
- The appointment of the Interim ISSO should be documented with a formal designation letter. Ultimately, a full time ISSO for the should be appointed and documented with a formal designation letter.

Access Controls

Access to programs and controls over data 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. Physically securing access includes keeping computers in locked rooms to limit physical access. Logical controls, such as security software programs, are designed to prevent or detect unauthorized access to sensitive files. Inadequate access controls diminish the reliability of data and increase the risk of unauthorized data modification, malicious or unintentional destruction of data, or inappropriate disclosure of information.

During FY 2007, CBP improved in the area of access to programs and data, specifically regarding . However, KPMG also identified additional issues. We noted significant access control vulnerabilities These are significant issues as personnel inside the organization who best understand the organization's systems, applications, and business processes have the ability to knowingly, or unknowingly, exploit these specific systems, applications, and powerful system utilities. Some of the vulnerable devices identified were used for . In some cases, users were able to access with group passwords, system default passwords, or the same passwords with which they logged As a result, unauthorized users could maliciously target to obtain information to attempt further access into CBP's .

2. Conditions noted regarding access controls were the following:

- A full listing of trade partners was never compiled to assess the full scope of the status of connections to . KPMG noted that a complete and accurate listing is still not maintained. Of those connections that have been accounted for, KPMG noted that only 7% of identified legacy connections had an interconnection security agreement (ISA) that has not expired. KPMG does note that a virtual private network (VPN) solution is being phased in and legacy connections are being phased out and that significant progress is being made to move all

existing trade partners to the new VPN solution, in which they will obtain an ISA documenting the connection.

- A centralized listing of contract personnel is not maintained, including employment status. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe accounts deleted. KPMG cannot acknowledge this list as representative of all terminated contractors, since terminated contract personnel may not have mainframe access or their access may not have been removed after their termination.
- Password parameters do not meet CBP or DHS policy.
- CBP policy is inconsistent with DHS policy. CBP's policy stated that sessions should automatically disconnect after 30 minutes of inactivity, which is not consistent with DHS policy. Also, CBP's policy stated that the workstation should log off from all connections after 5 minutes of inactivity. According to applicable guidance, all system connections do not need to be terminated after 5 minutes of inactivity on the workstation. CBP workstations could not enforce the activation of a password-protected screensaver after five minutes of inactivity. The settings could be disabled or changed by individual users.
- A solution has not been implemented to maintain audit logs for an appropriate period of time. Audit logs are not being reviewed for security violations for the .
- System accounts on the are given to users so they may perform their duties at CBP. When a user has not used the account for a specified period of time as noted in issued policies, that account should be disabled automatically by the system. During the course of FY 2007, this control was not adequately implemented.
- Deficiencies regarding control over physical data center access resulting from inadequate recertification performed for physical access to the data center.
- Audit logs of powerful system utilities are not maintained. KPMG reviewed the existence of logs for a selection of dates and noted that logs were not available for several of the selected dates. KPMG noted that within a 90-day window, complete logs were available for all selected dates except one. For the year-long window, 17 summary reports were unavailable.
- is currently configured to disable accounts after 90 days of inactivity. KPMG also noted that the job is configured to run weekly, which does not comply with the requirement for automatic disabling of accounts after 30 days of inactivity.
- has been adjusted to limit active emergency access to 24 hours after the request. KPMG notes, however, that the emergency table is still being used and that administrator or supervisory approval is not required each time emergency access is activated once an individual has been added to this emergency access table.
- There are currently no procedures in place for the completion of semi-annual recertifications of accounts. KPMG also noted that a recertification of accounts is not performed on a semi-annual basis.
- Several access control weaknesses for the VPN solution were found.
- The log indicating changes to a user's access in is not regularly reviewed by personnel independent from those individuals that made the changes.
- Evidence of the review of security violation logs for 6 of 25 dates was not available for review.
- Authorizations are not being maintained for personnel that have administrator access to Top Secret in the environment.
- Access control policies and procedures have not been formally documented for the . KPMG also noted that access authorization forms were not completed for 27 out of 45 accounts created in FY 2007.

- Procedures have been developed and a new termination form (CF-241) has been developed for use in terminating employees. However, these procedures were not implemented during the majority of the fiscal year.
- Multiple terminated employees retained active accounts on the . They were disabled as a result of accounts being inactive for 90 days. Therefore, these accounts were active 90 days after the employee terminated from CBP.
- Configuration management exceptions were identified on CBP domain controllers and hosts supporting the .
- Patch management exceptions were identified on CBP domain controllers and hosts supporting the .

Recommendations:

2. We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders consider the following actions:

   - CBP should identify all connections in place with the and account for each connection with a documented ISA.
   - CBP should continue to work towards implementation of a contractor employee tracking system. Deactivation of all systems access of terminated contractors should occur immediately upon separation from CBP. A listing of terminated contract personnel should be periodically distributed to information system administrators so they remove user access and periodically assess contractor access to CBP systems.
   - Configuration of password policies should reflect those set forth in CBP and DHS guidance. Also, configuration of password policies should reflect those set forth in CBP and DHS guidance.
   - CBP's automatic session disconnection policy should be modified to be consistent with DHS policy. CBP's policy should be modified to reflect that only the password-protected screensaver must be activated after 5 minutes of inactivity. CBP should continue deployment of Active Directory and Windows 2003 in order to establish and maintain group policy and enforce password-protected screensaver settings on the workstations.
   - CBP should configure the to maintain audit logs and track security events according to CBP and DHS policies. audit logs should be reviewed on a regular basis, according to CBP and DHS policy, to detect potential security events.
   - Administrators should implement a control to automatically disable or remove accounts after thirty days of inactivity in the system.
   - CBP should continue to work towards improving the recertification process followed for reviewing access to the data center. An access request form should be required before access is granted to the data center, as stated in CBP policies and procedures. Terminated employees' access should be removed immediately upon termination of the employee.
   - Complete and accurate records should be maintained of logs in accordance with CBP document retention policy. The logs should be reviewed regularly for suspicious activity in accordance with CBP policy.
   - The configuration for should be modified to disable accounts after 30 days of inactivity. The job schedule for the deactivation procedure should be modified to execute on a daily basis to minimize the time difference between the inactivity period and deactivation time.
   - Supervisory approval should be required each time a user requires activation of emergency access abilities on the . Regular recertifications of the emergency access table should be performed to ensure persons with the capability to request emergency access need to remain on the emergency access table.
   - Formal procedures should be developed outlining guidance for recertifying

accounts and access to shared data. Regular recertifications of accounts and access to shared data should be performed as required by the developed procedures.

- The VPN servers should be configured to store information about the creation dates and activity of users in order to be able to properly identify inactive accounts and allow for their deletion. The recertification process should be automated in order to remove the need for after the fact recertification via methods not documented in recertification procedures (email, verbal, etc.). The process of deactivating accounts at the end of the recertification period should be improved to ensure that all accounts that should be removed from the system are removed.
- Procedures should be formalized for reviewing access change logs. The review of these logs should be implemented on a periodic basis as set forth in CBP procedures.
- A periodic review of access violation logs should be performed for all systems.
- Procedures should be developed and implemented to restrict access to administrative capabilities. Documented and approved authorization requests should be required for each person needing access to the mainframe administrative capabilities.
- Access control policies and procedures should be developed and implemented for the Documented and approved authorization requests should be required for each person needing access to the .
- The recently developed procedures for completion of the employee termination forms should be implemented. System Security should be notified of all terminating employees so that systems access can be removed appropriately and timely.
- CBP should work to coordinate notices of termination of employees in a timely manner so that accounts can be deactivated immediately upon the departure of the employee.
- Corrective actions should be implemented to ensure that information systems that support the and other financial systems are configured to the security requirements outlined in DHS policy. Configurations that should be addressed include, but are not limited to: stronger password configurations, restrictions on access granted to ports on servers and audit log generation and maintenance.
- Corrective actions should be completed surrounding the vulnerabilities identified and implement policies and procedures to ensure that the information systems that support and maintain CBP financial data are secured with the most up to date and tested patches provided by vendors. Patches that have been validated as appropriate for CBP information systems should be applied to these systems to address the conditions noted.

Application Software Development and Change Controls

During FY 2007, we noted that CBP took corrective actions to address and close most prior year findings related to program changes. However, we identified additional findings related to program changes during our FY 2007 test work.

3. Conditions noted regarding program changes at CBP were the following:

- Developers can overwrite existing code in the development environment. The developer is able to extract the code from the development environment and place it into a personal folder on the user's personal computer. If multiple users are modifying a program in their own personal folders they may be overwriting existing changes.
- Controls over changes to the environment need improvement.
  - 3 out of 5 selected did not have post-implementation executive approval as required by the new OIT emergency change procedures.

  - 3 of the 15 selected changes to did not have formally documented test plans or test results.
  - None of the changes to showed evidence of review of the test results documented.
- Controls over changes to the need improvement.
  - 9 of the 20 changes to did not have formal test plans or documented results.
  - None of the changes to showed evidence of review of the documented test results.

Recommendations:

3. We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders consider the following actions:

   - Procedures should be implemented which prevent the overwriting of development code in the development environment.
   - Emergency change management post-implementation procedures should be constantly applied to all Furthermore, regular review of post-implementation procedures should occur. Regular feedback should be provided to change administrators to determine if any post-implementation steps may have been missed due to the expeditious nature of emergency changes.
   - CBP management OIT Change Control Board (CCB) and should ensure that all program offices appropriately document all test data, transactions, and program change results to monitor the quality of program changes.

System Software

During FY 2007, we noted that CBP took corrective actions to address and close one prior year finding related to system software. However, we identified additional findings related to system software during our FY 2007 test work.

4. Conditions noted regarding system software at CBP were the following:

   - Reviews of powerful system utilities are not conducted. While procedures are now in place for review of these logs, these procedures were not in place for the majority of the fiscal year.

Recommendations:

4. We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders consider the following actions:

   - Policies and procedures that have been developed for monitoring and reviewing logs of powerful system utilities for suspicious activity should be fully implemented.

Service Continuity

During FY 2007, we noted that CBP took corrective actions to address and close all prior year findings related to service continuity. However, we identified additional findings related to service continuity during our FY 2007 test work.

5. Conditions noted regarding service continuity at CBP were the following:

- Backup tapes did not have external labels affixed in order to indicate the sensitivity of the data contained in the tapes. Instead, containers in which the tapes are stored are labeled with media labels. Currently, CBP has obtained a waiver which relieves the responsibility to label media directly. However, because CBP is not in compliance with DHS policy, despite obtaining a waiver, the risk of CBP non-compliance still remains. If backup tapes were removed from the common container, there is still no indication of the sensitivity of the data on the tapes.
- Tape withdrawal requests were not documented.

Recommendations:

5. We recommend that the CBP CIO, in coordination with the CFO and other CBP functional leaders consider the following actions:

   - A method for labeling tapes should be developed that will not interfere with the tape library hardware.
   - Tape withdrawal requests should be monitored and logged to ensure that the withdrawal protocols are being appropriately followed.

APPLICATION CONTROL FINDINGS

During FY 2007, KPMG noted that a weakness in the drawback controls continues to exist within the . Specifically, does not support the tracking of drawback items to the line item level. Rather, only tracks drawbacks on a summary level. This control weakness was identified in FYs 2003, 2004, 2005, and 2006. This control weakness was presented to CBP management by the KPMG financial statement team as significant control weaknesses and also noted by the KPMG IT team.

Also, due to the design of , certain controls can be overridden without supervisory approval. For example, when a CBP entry specialist attempts to liquidate an import entry in , the system displays a warning message, indicating that a drawback claim had been filed against the import entry. However, entry specialists could override the warning message without supervisory review and process a refund without investigating pending drawback claims. The purpose of this warning message is to ensure that both a refund and drawback are not paid on the same goods. Entry specialists could override system edits designed to detect refunds exceeding the total duty, tax, and fees paid on an import entry. does not currently generate override reports for supervisory review.

In FY 2007, KPMG noted that there has been little change in the status of this finding. CBP is developing a control override report which will record all control overrides that have taken place for a period of time. Management stated that will not be implemented in FY 2007. KPMG concluded that a control mechanism to prevent overrides by specialists without supervisory approval would be an appropriate technical safeguard under application controls. Therefore, CBP should develop and implement a management review process of a control override report to facilitate independent review of any control overrides that take place. Ultimately, CBP should implement the appropriate controls in so that supervisory approval is required before a control override can occur.

MANAGEMENT COMMENTS AND OIG EVALUATION

We obtained written comments on a draft of this report from the CBP CIO. Generally, the CBP CIO 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 D.

In his response, the CBP CIO stated that CBP is:

- Taking steps to ensure that entity-wide security program planning and management controls are in place to establish a framework and continuing cycle of activity to manage security risk;
- Working to ensure that the assignment of sensitive functions is legitimate, that the weaknesses that can lead to a control override in certain systems is mitigated, and that physical and electronic access to sensitive CBP systems is secured and carefully monitored;
- Continuing to develop applicable policies and procedures to ensure that certain duties are separated, as necessary and to monitor user roles and new user or access requests to prevent future segregation of duty conflicts;
- Working to ensure that the [redacted] Continuity of Operations Plan (COOP) is as current as possible, and that the alternate processing site has the hardware and support necessary to continue operations in the event of an emergency; and
- Ensuring that proper separation of roles between the development and production environments are established.

OIG Response

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

APPENDIX A

DESCRIPTION OF KEY FINANCIAL SYSTEMS AND IT INFRASTRUCTURE WITHIN THE SCOPE OF THE FY 2007 CBP FINANCIAL STATEMENT AUDIT

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE

Below is a description of significant CBP financial management systems and supporting IT infrastructure included in the scope of CBP's FY 2007 Financial Statement Audit.

Locations of Review: The CBP .

Systems Subject to Review:

- is CBP's financial management system that consists of a 'core' system, which supports primary financial accounting and reporting processes, and a number of additional subsystems for specific operational and administrative management functions. is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the -based financial system using a phased approach.

- is a collection of business process -based systems used by CBP to track, control, and process all commercial goods, conveyances and private aircraft entering the U.S. territory for the purpose of collecting import duties, fees, and taxes owed to the Federal government. Key application software within includes systems for data input/output, entry and entry summary, and collection of revenue.

- – Used for tracking seized assets, Customs Forfeiture Fund, and fines and penalties.

APPENDIX B

FY 2007 NOTICES OF IT FINDINGS AND RECOMMENDATIONS

CBP FY 2007 IT NOTICES OF FINDINGS AND RECOMMENDATIONS RELATED TO FINANCIAL SYSTEM SECURITY

Notices of Findings and Recommendations – Definition of Risk Ratings:

The Notices 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 CBP's control environment and on the integrity of the financial data residing on the CBP'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.

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-07-01	Due to the design of , certain controls can be overridden without supervisory approval. For example, when a CBP entry specialist attempts to liquidate an import entry in , the system displays a warning message, indicating that a drawback claim had been filed against the import entry. However, entry specialists could override the warning message without supervisory review and process a refund without investigating pending drawback claims. The purpose of this warning message is to ensure that both a refund and drawback are not paid on the same goods. We also determined that entry specialists could override system edits designed to detect refunds exceeding the total duty, tax, and fees paid on an import entry. does not currently generate override reports for supervisory review. In FY 2007, we noted that there has been little change in the status of this	• Develop and implement a management review process of a control override report to facilitate independent review of any control overrides that take place. • Implement the appropriate controls in so that supervisory approval is required before a control override can occur.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	finding. CBP is developing a control override report which will record all control overrides that have taken place for a period of time. Management stated that [redacted] will not be implemented in FY 2007. We concluded that a control mechanism to prevent overrides by specialists without supervisory approval would be an appropriate technical safeguard under application controls.				
CBP-IT-07-02	A full listing of trade partners was never compiled to assess the full scope of the status of connections to [redacted]. We noted that a complete and accurate listing is still not maintained. Of those connections that have been accounted for, we noted that only 7% of identified legacy connections had an ISA that has not expired. A VPN solution is being phased in and legacy connections are being phased out and that significant progress is being made to move all existing trade partners to the new VPN solution, in which they will obtain an ISA documenting the connection.	Identify all connections in place with the [redacted] and account for each connection with a documented ISA.		**X**	**Medium**
CBP-IT-07-03	CBP does not maintain a centralized listing of contract personnel, including employment status. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe accounts deleted. We cannot acknowledge this list as representative of all terminated contractors, since terminated contract personnel may not have mainframe access or their access was not removed after their termination.	• Continue work towards implementation of a contractor employee tracking system. • Deactivate all systems access of terminated contractors immediately upon separation from CBP. • Periodically distribute a listing of terminated contract personnel to information system administrators so they remove user access and periodically assess contractor access to CBP systems.		**X**	**High**
CBP-IT-07-04	We confirmed that in FY 2007, backup tapes do not have external labels affixed in order to indicate the sensitivity of the data contained in the	Develop a method for labeling tapes that will not interfere with the tape library machinery.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	tapes. Instead, containers in which the tapes are stored are labeled with media labels. Currently, CBP has obtained a waiver which waives the responsibility to label media directly. However, CBP remains non-compliant and the risk still remains.				
CBP-IT-07-05	We noted the following issues related to password parameters: • minimum password length is set to six characters • Password complexity is not set on the • minimum password length is set to six characters • Password complexity is not set on the	• Configure password policies to reflect those set forth in CBP and DHS guidance. • Configure password policies to reflect those set forth in CBP and DHS guidance.		**X**	**High**
CBP-IT-07-06	We noted the following issues: • CBP's policy stated that sessions should automatically disconnect after 30 minutes of inactivity, which is not consistent with DHS policy. • CBP's policy stated that the workstation should log off from all connections after 5 minutes of inactivity. According to applicable guidance, all system connections do not have to be terminated after 5 minutes of inactivity on the workstation. • CBP workstations could not enforce the activation of a password-protected screensaver after five minutes of inactivity. The settings could be disabled or changed by individual users.	• Modify CBP's automatic session disconnection policy so that it is consistent with DHS policy. • Modify CBP policy to reflect that only the password-protected screensaver must be activated after 5 minutes of inactivity. • Continue deployment of and Windows 2003 in order to establish and maintain group policy and enforce password-protected screensaver settings on the workstations.		**X**	**Medium**
CBP-IT-07-07	We determined that does not have the ability to prevent developers from overwriting existing code in the development environment. The developer is able to extract the code from the development environment and place it into a personal folder on the user's personal computer. If multiple users are modifying a program in their	Implement procedures which prevent the overwriting of development code in the development environment.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	own personal folders they may be overwriting existing changes.				
CBP-IT-07-08	A solution has not been implemented to maintain [redacted] audit logs for an appropriate period of time. Audit logs are not being reviewed for security violations for the [redacted].	• Configure the [redacted] system to maintain audit logs and track security events according to CBP and DHS policies. • That [redacted] audit logs be reviewed on a regular bases, according to CBP and DHS policy, to detect potential security events.		**X**	**Medium**
CBP-IT-07-09	We noted that accounts are not deactivated automatically after 30 days of inactivity. Accounts are disabled for inactivity once a month using a manually initiated job.	Implement a control to automatically disable or remove accounts after thirty days of inactivity in the system.		**X**	**High**
CBP-IT-07-10	We reviewed the procedures and evidence of the most recent recertification performed for physical access to the data center. We noted the following: • Two people had access that was not appropriately documented with an approved access request form. • One terminated employee retained access after the recertification. • One user was marked to be removed as a result of the recertification but was not removed appropriately.	• Continue to work towards improving the recertification process. • Require an access request form before access is granted to the data center, as stated in policies and procedures. • Remove terminated employees' access immediately upon termination of the employee.		**X**	**Medium**
CBP-IT-07-11	CBP System Security does not consistently retain audit logs of powerful [redacted] system utilities. We reviewed the existence of [redacted] logs for a selection of dates and noted that logs were not available for a series of dates. We noted that within a 90 day window, complete logs were available for all selected dates except one. For the year long window, 17 summary reports were unavailable.	• Maintain complete and accurate records of [redacted] logs according to CBP document retention policy. • Regularly review the [redacted] logs for suspicious activity according to CBP policy.		**X**	**Medium**
CBP-IT-07-12	As identified in prior year issues	Ensure that [redacted]		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	reported in FY 2003, FY 2004, FY 2005 and FY 2006, we noted that improvements are still needed in CBP's Incident Handling and Response Capability which may potentially limit CBP's ability to respond to incidents in an appropriate manner. In FY 2007, we noted that [redacted] will not be installed on all workstations for the majority of the fiscal year.	is installed on all workstations under the control of CBP.			
CBP-IT-07-13	During test work around the application of security patches, we noted that a complete listing of workstations is not maintained by System Security. We noted that System Security does not have the ability to quickly compile a listing of all workstations under CBP's ownership.	• Work to eliminate the use of local workgroups and include all CBP workstations in a CBP administered domain. • Compile and regularly maintain a full and accurate listing of CBP workstations and use this list to monitor and maintain patch levels for all CBP workstations.	**X**		**Medium**
CBP-IT-07-14	We noted that tape withdrawal requests are not documented.	Monitor tape withdrawal requests that come from employees and log these requests to ensure that tape withdrawals are being completed appropriately.		**X**	**Low**
CBP-IT-07-15	We noted that the [redacted] is currently configured to disable accounts after 90 days of inactivity. We also noted that the job is configured to run weekly, which does not comply with the requirement for automatic disabling of accounts.	• Change the configuration for [redacted] to disable accounts after 30 days of inactivity. • Change the job schedule for the deactivation procedure to run on a daily basis to minimize the time difference between the inactivity period and deactivation time.		**X**	**High**
CBP-IT-07-16	We noted that the [redacted] has been adjusted to limit active emergency access to 24 hours after the request. We noted however that the emergency table is still being used and that	• Require supervisory approval each time a user requires activation of emergency access		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	administrator or supervisory approval is not required each time emergency access is activated.	abilities. • Perform regular recertifications of the emergency access table to ensure persons with the capability to request emergency access need to remain on the emergency access table.			
CBP-IT-07-17	CBP System Security does not conduct reviews of powerful system utilities. Specifically, the utilities [redacted] are not reviewed by management. Additionally, while procedures are now in place for review of these logs, these procedures were not in place for the majority of the fiscal year.	Implement policies and procedures that have been developed for monitoring and reviewing logs of powerful system utilities for suspicious activity.		**X**	**Medium**
CBP-IT-07-18	We noted there are currently no procedures in place for the completion of semi-annual recertifications of [redacted] accounts. We also note that a recertification of [redacted] accounts is not performed on a semi-annual basis.	• Develop formal procedures for recertifying [redacted] accounts and access to shared data. • Perform regular recertifications of [redacted] accounts and access to shared data as required by developed procedures.	**X**		**Medium**
CBP-IT-07-19	We noted that the completion of security awareness training is not appropriately tracked at CBP. We noted that out of a selection of 45 CBP employees, one employee maintained access to [redacted] without having completed the refresher security awareness training course. The individual completed an awareness course that was not the CBP-wide security awareness training required for all CBP employees.	• Ensure that security awareness training is completed in a timely manner by all employees with access to CBP information systems. • Continue to work towards implementing online training for all CBP personnel to facilitate automated tracking of the completion of security awareness training.		**X**	**Low**
CBP-IT-07-20	We noted several access control weaknesses for the VPN solution	• Automate the		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	during test work. Specifically, we noted: • The VPN sever does not maintain information on user account creation and inactivity and therefore cannot terminate inactive accounts or provide audit information regarding the creation of VPN accounts, • Accounts that did not recertify during the recertification time period or were marked for deletion during the recertification period remained active on the system after the accounts should have been deactivated by VPN administrators, • Procedures for recertifying accounts were not fully implemented and accounts were recertified by means beyond those identified in documented procedures	recertification process in order to remove the need for after-the-fact recertification via methods not documented in recertification procedures (email, verbal, etc.) • Configure the VPN servers to store information about the creation dates and activity of users in order to be able to properly identify inactive accounts and allow for their deletion. • Improve the process of deactivating accounts at the end of the recertification period and ensure that all accounts that should be removed from the system are removed.			
CBP-IT-07-21	We noted that when changes to a user's access are performed in [redacted], the log of these events is not regularly reviewed by personnel independent from those individuals that made the changes.	Formalize procedures for reviewing these access change logs and that review of these logs is implemented on a periodic basis as set forth in criteria.		**X**	**Medium**
CBP-IT-07-22	We noted that the following documents as not having documented approval and/or approval dates: • [redacted] – No approval for majority of fiscal year • Configuration Management Code Migration Procedures for [redacted] – No approval or effective date • Configuration Management Code Migration Procedures for [redacted] – No approval date or effective date • Production Management Team Procedures – No approval, no change history • [redacted] Operations: Standard	Implement procedures in OIT divisions to perform a review of all documentation to update, consolidate and approve the documented procedures in use by operational personnel.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Operating Procedures – No approval				
CBP-IT-07-23	3 out of 5 selected Emergency Changes did not have post-implementation Executive Approval as required by the new OIT emergency change procedures.	Consistently apply emergency change management post-implementation procedures to all emergency changes. Furthermore, post-implementation procedures should be regularly reviewed and provide regular feedback to change administrators to determine any post-implementation steps that may have been missed due to the expeditious nature of emergency changes.	**X**		**Medium**
CBP-IT-07-24	The recertification process has several weaknesses. Of the 45 selected ports, 45 ports none had formally documented communication between the responsible DFO and OFO headquarters as directed by the FY 2006 memorandum put out by Office of Finance.	• Apply procedures outlined in the newly distributed memorandum from Office of Field Operations dated April 27, 2007 • Consistently document results of recertifications at the port level and maintain documentation.		**X**	**Medium**
CBP-IT-07-25	We noted that the does not have an ISSO, but has been assigned an interim ISSO. We noted that the interim ISSO is not formally documented as the ISSO.	• Formally document the appointment of with a formal designation letter, and • Appoint a full time ISSO for the and document that appointment with a formal designation letter.	**X**		**Low**
CBP-IT-07-26	We noted that evidence of the review of security violation logs for 6 of 25 dates were not available for review.	Perform periodic review of access violation logs.	**X**		**Medium**
CBP-IT-07-27	We noted that authorizations are not being maintained for personnel that have administrator access to	• Develop and implement procedures to restrict access to	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		administrative capabilities, and • Require documented authorization requests and approval for each person requiring access to the [redacted] administrative capabilities.			
CBP-IT-07-28	We noted that access policies and procedures have not been formally documented for the [redacted]. We also noted that access authorization forms were not completed for 27 out of 45 accounts created in FY 2007.	• Develop and implement access policies and procedures for the [redacted] to document formal methods for requesting and approving access for the [redacted]. • Require documented authorization requests and approval for each person requiring access to the [redacted]	**X**		**Medium**
CBP-IT-07-29	We noted that procedures have been developed and a new termination form (CF-241) has been developed for use in terminating employees. While these procedures address the submission of the form to System Security and require notification of removal of system access from System Security, the new procedures were developed and activated in June, 2007. The procedures are currently not implemented, however.	• Implement the recently developed procedures for completion of the termination forms and notify System Security for all terminating employees so that systems access can be removed appropriately.		**X**	**Medium**
CBP-IT-07-30	We noted that multiple terminated employees retained active accounts on the [redacted]. They were disabled as a result of accounts being inactive for 90 days. Therefore, these accounts were active 90 days after the employee terminated from US CBP.	• Work with other US CBP Offices and within OIT to receive notice of termination of employees in a timely manner so that accounts can be deactivated on the departure of the employee. • Terminate accounts for terminated employees in a timely manner.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-07-31	We noted that 12 of the 45 selected ports/headquarters did not have self inspection worksheets completed. Accordingly, we were not able to determine whether specific high risk combinations of roles were performed at these ports/headquarters.	• Apply procedures outlined in the newly distributed memorandum from Office of Field Operations • Consistently document results of recertifications at the port level.		**X**	**Medium**
CBP-IT-07-32	We selected 20 out of 201 changes and noted the following: • 9 of the 20 changes did not have formal test plans or documented results • None of the changes showed evidence of review of the documented test results.	Ensure that all program offices appropriately document all test data, transactions, and program change results.	**X**		**Medium**
CBP-IT-07-33	We selected 15 of 90 changes and noted the following: • 3 of the 15 selected changes did not have formally documented test plans or test results. • None of the changes showed evidence of review of the test results documented.	Ensure that all program offices appropriately document all test data, transactions, and program change results to monitor the quality of program changes.	**X**		**Medium**
CBP-IT-07-34	We noted that virus protection is not installed on all CBP workstations. Specifically, we noted at the time of testing that approximately 6,000 of CBP's approximate 38,000 workstations do not have antivirus protection installed. Since the initial testing was performed, we noted that immediate remediation has begun and as of September 28, 2007, improvements have been made but 1,557 out of 42,429 workstations still are missing virus protection software.	Ensure that antivirus protection is installed on all workstations under the control of CBP.	**X**		**High**
CBP-IT-07-35	During our technical testing, eighteen configuration management exceptions were identified Domain Controllers and hosts supporting the application.	Implement corrective actions to ensure that information systems that support the application and other financial systems are configured to the security requirements outlined in DHS policy. Configurations		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		that should be addressed include, but are not limited to: stronger password configurations, restrictions on access granted to ports on servers and audit log generation and maintenance.			
CBP-IT-07-36	During our technical testing, thirty-seven patch management exceptions were identified on [redacted] Domain Controllers and hosts supporting the [redacted] application.	Complete corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the information systems that support and maintain CBP financial data are secured with the most up to date and tested patches provided by vendors. Patches that have been validated as appropriate for CBP information systems should be applied to these systems to address the conditions noted.		**X**	**High**

APPENDIX C

STATUS OF PRIOR YEAR NOTICES OF FINDINGS AND RECOMMENDATIONS AND COMPARISON TO CURRENT YEAR NOTICES OF FINDINGS AND RECOMMENDATIONS

STATUS OF PRIOR YEAR CBP IT NOTICES OF FINDINGS AND RECOMMENDATIONS

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-06-01	Due to the design of , certain controls can be overridden without supervisory approval. For example, when a CBP entry specialist attempts to liquidate an import entry in , the system displays a warning message, indicating that a drawback claim had been filed against the import entry. However, entry specialists could override the warning message without supervisory review and process a refund without investigating pending drawback claims.		Reissued See CBP-IT-07-01
CBP-IT-06-02	CBP management has not established ISAs for legacy connections with . Additionally, the majority of financial institutions connecting with do not have ISAs.		Reissued See CBP-IT-07-02
CBP-IT-06-03	CBP management has not performed a formal certification and accreditation on the as a whole. Specifically, a formal security control assessment and a formal risk assessment have not been performed for components of the	**X**	
CBP-IT-06-04	CBP does not maintain a centralized listing of separated contract personnel. The only method CBP employs to track terminated contractors is the use of a report of users that had their account deleted.		Reissued See CBP-IT-07-03
CBP-IT-06-05	CBP management has not performed a formal review of individuals with physical access to the data center. Additionally, CBP management has not established formal procedures for revoking physical access to buildings.		Reissued See CBP-IT-07-10
CBP-IT-06-06	CBP has not performed a separate certification and accreditation for the applications remaining in the seven business process areas defined in the Administrative Applications C&A.	**X**	

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-06-07	does not have an automated mechanism to detect and deactivate users that have not logged on for 90 days per DHS policy.	**X**	
CBP-IT-06-08	Field offices are not consistently reporting the completion of recertifications at their ports to the OFO headquarters. Email confirmation of completion of recertifications were not available for Boston, Baltimore, New Orleans, Miami, and Calgary (Canada) field offices, and the Los Angeles field office only provided an email stating that recertification process exists, but did not confirm that recertifications had been completed.		Reissued See CBP-IT-07-24
CBP-IT-06-09	We could not obtain the requested evidence of recertifications from CBP for any of the 44 selected field level ports to determine whether accounts with sensitive and high-risk combination of functions are reviewed for appropriateness.		Reissued See CBP-IT-07-31
CBP-IT-06-10	Improvements are still needed in CBP's Incident Handling and Response Capability which may potentially limit CBP's ability to respond to incidents in an appropriate manner. Specifically, we noted the following issues: • will not be installed on all workstations for the majority of the fiscal year. • 3 of 8 selected system flaw notifications did not have an associated Service Center ticket.		Reissued See CBP-IT-07-12
CBP-IT-06-11	We noted that the process for deletion of accounts for terminated government and contractor personnel may be utilizing erroneous data. Specifically, we noted that the files being sent from the Security group to the Security team to terminate accounts of separated employees do not display the true status of employees. The query producing the separated contractor file	**X**	

NFR No.	Description	Disposition	
		Closed	Repeat
	includes individuals with accounts that have been locked after 30 days of inactivity. Additionally, the separated government employees file is not accurate as many government employees are separated and return to CBP as contractors. Consequently, the Security Group does not deactivate the accounts for these instances.		
CBP-IT-06-12	We noted that 24 out of 45 selected individuals did not have formally documented VPN access authorization forms. Additionally, CBP has not implemented formal procedures for VPN recertification for the majority of FY 2006.		Reissued See CBP-IT-07-20
CBP-IT-06-13	CBP System Security does not conduct reviews of powerful system utilities. Specifically, management does not review the utilities		Reissued See CBP-IT-07-17
CBP-IT-06-14	Multiple methods of termination of accounts are used by Systems Security personnel (i.e. electronic mail, phone calls, and termination checklists). We selected 45 terminated employees to determine whether termination checklists had been consistently completed. Of the 45 employees, only 30 forms were provided. Of these 30 forms, we noted that 9 out of 30 forms did not have supervisory signature, which signifies completion of the form to include notification sent to System Security for removal of logical access to applications. We noted that termination checklists (CF-241) are not consistently completed for separating employees throughout the organization.		Reissued See CBP-IT-07-29
CBP-IT-06-15	Backup tapes do not have affixed external labels to indicate the sensitivity of the data contained in the tapes.		Reissued See CBP-IT-07-04
CBP-IT-06-16	CBP System Security does not have formal policies and procedures in place		Reissued See CBP-IT-07-17

NFR No.	Description	Disposition	
		Closed	Repeat
	for monitoring powerful/sensitive system utilities.		
CBP-IT-06-17	Improvements still needed in CBP's technical security controls. Related to issues reported in FY02, FY03 and FY04 findings regarding host and network based security system access deficiencies, we noted the following: • CBP has confirmed that they will not be implementing the Passfilt.dll system control program to enforce strong passwords or the Windows password protection feature enhancement upgrade referred to as • CBP has not made the configuration changes to the Windows that was compromised in FY03 intrusion tests. • Discovered key systems' domains in targeting for potential unauthorized access attempts where we were able to identify major CBP network domains. • Exploited a system vulnerability that had not been corrected. • We confirmed that the number of Domain Administrators on selected Domains has increased since 2005. • ESM identified weak passwords, expired passwords, misconfigurations, and missing patches. • Identified vulnerabilities on an Oracle database which had critical patches missing, weak passwords and auditing is not enabled.		Reissued See CBP-IT-07-35 and CBP-IT-07-36
CBP-IT-06-18	We noted the following issues related to password parameters: • minimum password length is set to six characters. • minimum password length is set to six characters. • Password complexity is not set on		Reissued See CBP-IT-07-05

NFR No.	Description	Disposition	
		Closed	Repeat
	the . • Password complexity is not set on . • Password complexity is not set on the .		
CBP-IT-06-19	We noted the following issues related to automatic session disconnection: • CBP's policy states that sessions should be automatically disconnected after 30 minutes of inactivity, which is not consistent with DHS' policy. • CBP's policy states that the workstation should log off from all connections after 5 minutes of inactivity, which is a documentation error. According to applicable guidance, all system connections do not have to be terminated after 5 minutes of inactivity on the workstation. • sessions are configured to terminate after 60 minutes of inactivity. • CBP workstations cannot enforce the activation of a password-protected screensaver after 5 minutes of inactivity. The settings can be disabled or changed by individual users.		Reissued See CBP-IT-07-06
CBP-IT-06-20	is not configured to disable user accounts after 3 consecutive failed logon attempts. Additionally, per observation, we noted accounts were not locked after three consecutive failed login attempts.	**X**	
CBP-IT-06-21	CBP does not document formal approval of system changes for the system. We selected 8 regularly scheduled changes to determine if formal approval was given and documented. Per inspection of documentation, we were informed that there is no formally	**X**	

NFR No.	Description	Disposition	
		Closed	Repeat
	documented approval for the 8 selected changes.		
CBP-IT-06-22	We noted weaknesses related to the deposit and withdrawal of backup tapes: • Tape deposit receipts for 2 of 25 selected dates were not available. • Withdrawal of backup tapes from the off-site storage facility is not logged.		Reissued See CBP-IT-07-14
CBP-IT-06-23	CBP System Security does not consistently retain audit logs of powerful mainframe system utilities. Specifically, we selected 25 reports to determine if powerful system utilities are being consistently logged. We determined that 5 out of the 25 selected logs were missing.		Reissued See CBP-IT-07-11
CBP-IT-06-24	We determined that does not have the ability to prevent developers from overwriting existing code in the development environment. The developer is able to extract the code from the development environment and place it into a personal folder on the user's personal computer. If multiple users are modifying a program in their own personal folders they may be overwriting existing changes.		Reissued See CBP-IT-07-07
CBP-IT-06-25	Accounts are not deactivated after 90 days of inactivity with respect to the system. We determined through inspection of audit evidence acquired from that the defined deactivation period is, in fact, 180 days.		Reissued See CBP-IT-07-15
CBP-IT-06-26	Security Administrators do not keep audit logs for the prescribed period of time. Audit logs are only available for, at the most, the past three months. Logs are not maintained beyond the configured space for the log file. We also noted that Security Administrators do not review audit logs.		Reissued See CBP-IT-07-08

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-06-27	We noted that accounts are not deactivated after 90 days of inactivity on the . We determined that the removal of inactive accounts is a manual process.		Reissued See CBP-IT-07-09
CBP-IT-06-28	are not fully documented for . The ISA documenting the connection between America and CBP is currently out of date. In addition, the connection that exists between Treasury and CBP is currently not officially documented.	**X**	
CBP-IT-06-29	The documentation of completed initial security awareness training is not properly maintained. We selected security awareness training documentation for 45 users. Per inspection of documentation, 13 of 45 did not have security awareness training certificates documented.		Reissued See CBP-IT-07-19
CBP-IT-06-30	Contractor access request forms for the could not be adequately tested. We noted that no list of contractors hired to work at CBP is maintained. Accordingly, audit procedures requiring a sample of contractor access request forms could not be requested.		Reissued See CBP-IT-07-03
CBP-IT-06-31	has excessive access to emergency processing capabilities. We noted that after an initial authorization to be added to an emergency user table in , a user can repeatedly request that their emergency access be reinstated, without being reauthorized. While emergency access in can expire in no more than nine days, some users renew their emergency access every nine days. We noted that CBP has not implemented an effective method of controlling this access, as users are not required to reauthorize their emergency access each time it is requested.		Reissued See CBP-IT-07-16
CBP-IT-06-32	Access change audit logs are not reviewed in . CBP		Reissued See CBP-IT-07-21

NFR No.	Description	Disposition	
		Closed	Repeat
	management does not independently review the changes that are put into place by the [redacted] security administrators.		
CBP-IT-06-34	Four [redacted] administrators share an administrator account on the [redacted]	**X**	
CBP-IT-06-36	We determined that the following documents have not been formally approved: • [redacted] – No approval. • Configuration Management Code Migration Procedures for [redacted] has no authorization. • Acquisition Planning and Selection and Development Process has no authorization. • Configuration Management Code Migration Procedure for Systems, Applications, and Products has no authorization. • Production Management Team Procedures – No approval, no change history. • [redacted] Operations: Standard Operating Procedures – No approval.		Reissued See CBP-IT-07-22
CBP-IT-06-37	User acceptance testing for [redacted] Remedy was not formally documented.	**X**	
CBP-IT-06-38	We noted that one individual with [redacted] administrator privileges did not have justified access. We noted that there are instances where [redacted] locks security administrator accounts due to various reasons that do not require documented approvals for reinstating the user account. Additionally, we noted that instances where the [redacted] security administrator is new or reinstatement of	**X**	

NFR No.	Description	Disposition	
		Closed	**Repeat**
	suspended/deleted accounts is needed, a documented approval is required. We noted that due to a system limitation within , management cannot produce a system-generated list of field security administrators that differentiates between the two cases.		
CBP-IT-06-39	We noted that 1 out of 3 job schedule changes did not have documented approval.	**X**	

Appendix D

Management Response to Draft CBP IT Management Letter

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

MAR 5 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Ken Ritchhart
Acting Assistant Commissioner
Office of Information and Technology

SUBJECT: Draft Audit Report - Information Technology Management Letter for the FY 2007 CBP Financial Statement Audit

This is in reply to your memorandum dated February 7, 2008 requesting written comments on the draft report and responses to the recommendations that are included in the subject IT Management letter. OIT would like to provide the following comments on the CBP actions that are being performed for the findings and recommendations from the FY 2007 audit.

Entity-wide Security Program Planning and Management
CBP concurred with KPMG's recommendations in this area. Steps have been taken to ensure that entity-wide security planning and management controls are in place to manage security risks. These steps include regular security risk assessments, a complete inventory of CBP workstations with the deployment of Tivoli Health Endpoint and antivirus protection to all workstations, security awareness training, and the documentation of re-certifications at the port level. Plans of Actions and Milestones (POAM) have been implemented for the Notices of Finding and Recommendation (NFR) and their status is provided in the attachment.

Access Controls

CBP concurred with KPMG's recommendations in this area. Steps have been taken to ensure that interconnection security agreements (ISA) are in place, that the assignment of sensitive functions is controlled, that any control override weaknesses in the CBP systems are mitigated, and that both physical and electronic access to sensitive systems is secured and monitored. POAMs have been implemented for NFRs and their status is provided in the attachment.

System Software

CBP concurred with KPMG's recommendations in this area. Steps have been taken to ensure that the policies and procedures which have been developed for monitoring audit logs are fully implemented. POAMs have been implemented for the NFRs and their status is provided in the attachment.

Service Continuity

CBP concurred with KPMG's recommendations in this area. Steps have been taken to ensure appropriate labeling of all computer peripheral media and the formalizing of media withdrawal requests. POAMs have been implemented for the NFRs and their status is provided in the attachment.

Application Software Development and Change Control

CBP concurred with KPMG's recommendations in this area. Separation of roles between development and production environments has been established. codes have been configured for the "Productive" setting, while configuration management and change control measures are continually upgraded. POAMs have been implemented for the NFRs and their status is provided in the attachment.

Thirty-six NFRs that addressed fifty-nine separate recommendations were created during the FY 2007 audit of which twenty-five were reissues of FY 2006 findings and eleven were new. Three of the thirty-six have been transferred to non-OIT groups, the Office of Finance (OF) and the Office of Field Operations (OFO) for remediation, and CBP action plans have been provided for the remaining thirty-three. For the latter thirty-three, CBP actions have been totally completed for nineteen and partially completed for an additional six. The corrective actions for thirty five recommendations have been completed, all of which are awaiting closure pending KPMG review. POAMs have been implemented for the NFRs and their status is provided in the attachment.

If you have any questions concerning this response, please contact Judy Wright, Office of Information and Technology Audit Liaison, at (703) 286-4155.

Attachments:

CBP FY 2007 IT Notices of Finding and Recommendation

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-01	In FY 2007, KPMG noted that there has been little change in the status of this finding. CBP is developing a control override report which will record all control overrides that have taken place for a period of time. Management stated that [redacted] will not be implemented in FY 2007. We concluded that a control mechanism to prevent overrides by specialists without supervisory approval would be an appropriate technical safeguard under application controls.	1.Develop and implement a management review process of a control override report to facilitate independent review of any control overrides that take place. 2.Implement the appropriate controls in [redacted] so that supervisory approval is required before a control override can occur. .	CBP concurs with the finding. A report is being created in [redacted] to identify entry summaries with refunds of duty with drawback that have been overridden and paid. The review of the report provides oversight of the compliance with warning messages on [redacted] returns of refunds with possible drawback claims. This oversight will help prevent CBP from paying duty refunds and also paying drawback claims of 99% duty. Supervisors will be required to review the report on a monthly basis to control overrides of the refunds paid that may also have drawback claims. This new report was implemented by 30 Sept 2007. [redacted] requirements will include management oversight functionality to require supervisory approval of the override, which prevents payment of duty refunds on entry summaries that have drawback claims.		X	1B-7/31/2008	1A-10/2/2007	High

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-02	This is a system-level finding. A full listing of trade partners was never compiled to assess the full scope of the status of connections to KPMG noted that a complete and accurate listing is still not maintained. Of those connections that have been accounted for, KPMG noted that only 7% of identified legacy connections had an that has not expired. KPMG does note that a VPN solution is being phased in and legacy connections are being phased out and that significant progress is being made to move all existing trade partners to the new VPN solution, in which they will obtain an ISA documenting the connection.	Identify all connections in place with the and account for each connection with a documented ISA.	CBP concurs with the finding. The Virtual Private Network (VPN) solution pilot from last year is now operational as of April 30, 2006. All new users are required to use the VPN solution. All legacy 'dial-up' connections are scheduled for migration to the VPN solution by the end of the fiscal year. CBP will also continue to utilize the new process on all identified connections. The NFR stated, "Of those connections that have been accounted for, KPMG noted that only 7% of identified connections had an ISA that has not expired. The correct number is currently 35%. The VPN migration with the use of the process will result in an efficient, maintainable, and repeatable solution that enhances both e-Government and security.		X	2B-3/31/2008	2A-10/09/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-03	This is a component-level finding. CBP does not maintain a centralized listing of contract personnel, including employment status. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe accounts deleted. KPMG cannot acknowledge this list as representative of all terminated contractors, since terminated contract personnel may not have access or their access was not removed after their termination.	Continue work towards implementation of a contractor employee tracking system. 1.Deactivate all systems access of terminated contractors immediately upon separation from CBP. 2.Periodically distribute a listing of terminated contract personnel to information system administrators so they remove user access and periodically assess contractor access to CBP systems.	CBP concurs with the finding. a: CBP is continuing to work towards the implementation of a contractor employee tracking system. b/c: CBP is presently in the process of identifying requirements for the automated contractor tracking system. The primary purpose of the tracking system will be to facilitate deactivation of separated contractor system accesses. The tracking system will also have the capability to create a listing that system administrators can use to periodically remove and assess contractor access to CBP systems. It is anticipated that the above actions will occur on or before September 30, 2007.		X		3A-10/12/2007 3B-10/12/2007 3C-10/12/2007	High

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-04	This is a component-level finding. KPMG confirmed that in FY 2007, backup tapes do not have external labels affixed in order to indicate the sensitivity of the data contained in the tapes. Instead, containers in which the tapes are stored are labeled with media labels. Currently, CBP has obtained a waiver which waives the responsibility to label media directly. However, CBP remains non-compliant and the risk still remains.	KPMG reviewed the POA&M and believes that work should continue to develop a method for labeling tapes that will not interfere with the tape library machinery.	CBP concurs with the findings. However as of this date, we do not have a method of labeling the tapes that does not require the use of adhesives. We had acquired the waiver because of the potential harm to our [redacted] by affixing adhesive in close proximity to the tape media. We will continue to research other methods and technologies of tape labeling that do not use adhesives.		X		9/28/2007	Low
CBP-IT-07-05	This is a system-level finding. KPMG noted the following issues related to password parameters: - [redacted] minimum password length is set to six characters - Password complexity is not set on the [redacted] minimum password length is set to six characters - Password complexity is not set on the [redacted]	1.Configure [redacted] password policies to reflect those set forth in CBP and DHS guidance. 2.Configure [redacted] password policies to reflect those set forth in CBP and DHS guidance.	CBP concurs with the finding. a. CBP is currently working to implement system and application software changes to support DHS password standards – targeted completion July 2007. b. CBP is currently implementing [redacted] with this roll out set to be completed by 12/31/07. As user accounts are migrated, complex passwords based on DHS standards are implemented. Current compensating controls that are in place: Secure network and [redacted] on Primary domain controllers.		X		5A – 1/8/2008 5B – 1/3/2008	High

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-06	This is a system-level finding. KPMG noted the following issues: - CBP's policy stated that sessions should automatically disconnect after 30 minutes of inactivity, which is not consistent with DHS policy. - CBP's policy stated that the workstation should log off from all connections after 5 minutes of inactivity. According to applicable guidance, all system connections do not have to be terminated after 5 minutes of inactivity on the workstation. - CBP workstations could not enforce the activation of a password-protected screensaver after 5 minutes of inactivity. The settings could be disabled or changed by individual users.	1.Modify CBP's automatic session disconnection policy so that it is consistent with DHS policy. 2.Modify CBP policy to reflect that only the password-protected screensaver must be activated after 5 minutes of inactivity. 3.Continue deployment of [redacted] and Windows 2003 in order to establish and maintain group policy and enforce password-protected screensaver settings on the workstations.	CBP concurs with the findings. a. Appendix E, E 5 Automatic Session Lockout of CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400 05C will be revised to state that "any mainframe session that has remained idle for at least 20 minutes will disconnect automatically." b. Section 5.5.1 Desktop Computer Practices of CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400 05C, will be revised to state that screensavers should activate after not more than 5 minutes of inactivity. c. CBP will continue the deployment of Active Directory and Windows 2003 Server in order to set up group policy and enforce password protected screensaver settings. Target due date December 31, 2007.		X	6C-3/31/2008	6A-7/11/2007 6B-7/11/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-07	This is a system level finding. KPMG determined that [redacted] does not have the ability to prevent developers from overwriting existing code in the development environment. The developer is able to extract the code from the development environment and place it into a personal folder on the user's personal computer. If multiple users are modifying a program in their own personal folders they may be overwriting existing changes.	CBP management implement procedures which prevent the overwrite of development code in the development environment.	CBP Concurs with the NFR. Management is developing two options for resolving this NFR. Once management selects the option and identifies the necessary funding, work can begin with an estimated completion date of 12/31/07.		X		10/18/2007	Medium
CBP-IT-07-08	This is a system-level finding. A solution has not been implemented to maintain [redacted] audit logs for an appropriate period of time. Audit logs are not being reviewed for security violations for the [redacted].	1.The [redacted] system be configured to maintain audit logs and track security events according to CBP and DHS policies. 2. [redacted] audit logs be reviewed on a regular bases, according to CBP and DHS policy, to detect potential security events.	CBP concurs with the finding. This is an ongoing project that is currently on hold awaiting funds to purchase equipment. Once the new equipment is in place, then all the servers will be configured to store logs centrally. Plans and procedures will be provided to administrators on reviewing log activity. Compensating controls that are currently in place include some audit logs from environment that are currently stored in a central location [redacted] that are installed on our primary domain controllers.		X	8A - 4/30/2008 8B - 1/3/2008		Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-09	This is a system-level finding. KPMG noted that accounts are not deactivated automatically after 30 days of inactivity. Accounts are disabled for inactivity once a month using a manually initiated job.	Administrators implement a control to automatically disable or remove accounts after thirty days of inactivity in the system.	CBP concurs with the NFR. For CBP will change the automatic disabling of inactive accounts from 90 days to 30 days. Target due date – 8/31/07		X		1/3/2008	High

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-10	This is a component level finding. KPMG reviewed the procedures and evidence of the most recent recertification performed for physical access to the data center. KPMG noted the following: - Two people had access that was not appropriately documented with an approved access request form. - One terminated employee retained access after the recertification. - One user was marked to be removed as a result of the recertification but was not removed appropriately.	1.Continue to work towards improving the recertification process. 2.Require an access request form before access is granted to the data center, as stated in policies and procedures. 3.Remove terminated employees' access immediately upon termination of the employee.	CBP concurs with the finding. a. CBP is continuing to work towards improving the recertification process. All corrective actions recommended by KPMG have been implemented to improve the recertification process. CBP implemented a new measure in May 2007 requiring the use of the "Two Person Rule" to ensure that oversights and human error do not occur. b. CBP continually uses for the requesting and granting of RA access. In the instance cited, a was not required for the security guard supervisor because he requires access for emergency reasons and cannot be denied Computer Room access. CBP will ensure that a is submitted to owners in future such cases as a courtesy measure. c. CBP currently has documented procedures within the Handbook, V. 1, dated March 2007, as well as CBP directives that govern the separation of CBP employees and contractors from CBP service.		X		10A-11/28/2007 10B-11/28/2007 10C-11/28/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-11	This is a system-level finding. CBP System Security does not consistently retain audit logs of powerful utilities. KPMG reviewed the existence of logs for a selection of dates and noted that logs were not available for a series of dates. KPMG noted that within a 90 day window, complete logs were available for all selected dates except one. For the year long window, 17 summary reports were unavailable.	1.Maintain complete and accurate records of logs according to CBP document retention policy. 2.Regularly review the logs for suspicious activity according to CBP policy.	CBP concurs with this finding. Per current policy, printed reports are kept for 90 days. The Security Operations team will ensure that all audit logs are retained for the 90-day period. Log Reviews and the resultant summary status reports have not been done by the ISSO due to the volume of records to review. The team is working on creating a Web-based application that automates the generation of audit log summary reports. This new application will enable the ISSO to quickly generate a Log Review summary report. Anticipated completion date of this new Web-based application is October, 2007. Online audit logs are maintained for a period of seven (7) years per the current Audit Retention Policy, CBP HB 1400-05C of the Security Handbook.		X	11A-6/30/2008	11B-1/28/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-12	This is a component-level finding. As identified in prior year issues reported in FY 2003, FY 2004, FY 2005 and FY 2006, KPMG noted that improvements are still needed in CBP's Incident Handling and Response Capability which may potentially limit CBP's ability to respond to incidents in an appropriate manner. In FY 2007, we noted that [redacted] will not be installed on all workstations for the majority of the fiscal year.	CBP ensure that [redacted] is installed on all workstations under the control of CBP.	CBP concurs with the NFR. The solution is a work in progress to be implemented by October 1, 2007: - Windows XP standard image incorporates [redacted] functionality. - Systems installed with this image will be patched according to CBP standards. - CBP has an auto-remediation capability to detect systems in Windows Domains that are issued dynamic IP addresses. - CBP will detect non-[redacted] and will install [redacted] Code based on Domain Member and dynamic (or leased) IP Address Targeted completion October 1, 2007. Continual improvement of this methodology is anticipated as this capability is deployed.		X		2/19/2008	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-13	This is a component-level finding. During test work around the application of security patches, KPMG noted that a complete listing of workstations is not maintained by System Security. We noted that System Security does not have the ability to quickly compile a listing of all workstations under CBP's ownership.	1.Work to eliminate the use of local workgroups and include all CBP workstations in a CBP administered domain. 2.Compile and regularly maintain a full and accurate listing of CBP workstations and use this list to monitor and maintain patch levels for all CBP workstations.	CBP concurs with this finding. a. Mitigations are currently in place through a group policy, workstations in [redacted] are required to run the [redacted] health" code Additionally, the CBP desktop build contains pre-staged [redacted] health code and antivirus software that will check for updates daily. b. Corrective action will be taken to develop, test, and implement a [redacted]-integrated system that will determine desktop network identification. Target completion date (for implementation): December 31, 2007. The solution requires an updated policy and technical change.	X		13A-4/30/2008 13B-3/29/2008		Medium
CBP-IT-07-14	This is a component-level finding. KPMG noted that tape withdrawal requests are not documented.	CBP monitor tape withdrawal requests that come from employees and log these requests to ensure that tape withdrawals are being completed appropriately.	CBP concurs with the finding and will take the following actions: 1.Create an online log for unscheduled tape recalls from the offsite storage facility [redacted] This process will be completed by July 31, 2007. 2. [redacted] will be updated to reflect the new logging procedure. This update will be completed by July 31, 2007.		X		11/28/2007	Low

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-15	This is a system-level finding. KPMG noted that the [redacted] is currently configured to disable accounts after 90 days of inactivity. KPMG also noted that the job is configured to run weekly, which does not comply with the requirement for automatic disabling of accounts.	2.Change the configuration for [redacted] to disable accounts after 30 days of inactivity. 2.Change the job schedule for the deactivation procedure to run on a daily basis to minimize the time difference between the inactivity period and deactivation time.	CBP concurs with this finding. ACS Security will work with the [redacted] programmers to have the ACS code changes made, tested, and user-approved in order to comply with the 30-day inactivity rules per DHS 4300A Sensitive Systems Handbook v3.3. Estimated target date for completion of the coding changes is January 31, 2008		X		15A-11/28/2007 15B-11/28/2007	High
CBP-IT-07-16	This is a system-level finding. KPMG noted that the [redacted] has been adjusted to limit active emergency access to 24 hours after the request. KPMG notes however that the emergency table is still being used and that administrator or supervisory approval is not required each time emergency access is activated.	1.Require supervisory approval each time a user requires activation of emergency access abilities. 2.Perform regular re-certifications of the emergency access table to ensure persons with the capability to request emergency access need to remain on the emergency access table.	CBP concurs with this finding. After careful review of the current Emergency Access Policy, CBP has decided to update the language to be compliant with the recommendations. Once the policy has been updated, CBP will take steps to implement procedures to satisfy the recommendations		X	16B - 5/15/2008	16A - 9/6/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-17	This is a system-level finding. CBP System Security does not conduct reviews of powerful system utilities. Specifically, the utilities [redacted] are not reviewed by management. Additionally, while procedures are now in place for review of these logs, these procedures were not in place for the majority of the fiscal year.	CBP management implement policies and procedures that have been developed for monitoring and reviewing logs of powerful system utilities for suspicious activity.	As of August 1, 2007, the [redacted] ISSO has implemented policies and procedures that have been developed for monitoring and reviewing logs of powerful system utilities for suspicious activities. These logs are identified in NFR-07-11 recommendation b. The [redacted] ISSO will continue to review the logs and report any anomalies as they occur.		X		11/28/2007	Medium
CBP-IT-07-18	This is a system-level finding. KPMG noted there are currently no procedures in place for the completion of semi-annual re-certifications of [redacted] accounts. KPMG also notes that a recertification of [redacted] accounts is not performed on a semi-annual basis.	1.Develop formal procedures for recertifying [redacted] accounts and access to shared data. 2.Perform regular re-certifications of [redacted] accounts and access to shared data as required by developed procedures.	CBP will determine a method for conducting semi-annual re-certifications of [redacted] accounts. This will involve analysis to determine the most feasible tools and methods for identifying the accounts, notifying the users, and validating that the accounts are still valid. The analysis will be completed by October 2007 with the implementation and first recertification to occur by September 2008.	X		18A - 9/1/2008 18B - 9/1/2008		Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-19	This is a component level finding. KPMG noted that the completion of security awareness training is not appropriately tracked at CBP. KPMG noted that out of a selection of 45 CBP employees, one employee maintained access to [redacted] without having completed the refresher security awareness training course. The individual completed an awareness course that was not the CBP-wide security awareness training required for all CBP employees.	1.Ensure that security awareness training is completed in a timely manner by all employees with access to CBP information systems. 2.Continue to work towards implementing online training for all CBP personnel to facilitate automated tracking of the completion of security awareness training.	CBP concurs with the finding. -CBP will work towards ensuring the on-line Virtual Learning Center (VLC) is the primary tool for completing and tracking Security Awareness Training. Issues concerning possession of a valid CBP email address to register in the VLC should be resolved when the system is upgraded on 8/3/07. This upgrade allows the ability to create temporary accounts that will merge with the employees' permanent accounts once established. - A conversion from Lotus to Active Directory Exchange, scheduled for completion by 12/31/07, should resolve additional VLC account issues. [redacted] will work with the OTD to establish controls that prevent employees from completing other Security Awareness courses if the basic course date is expired or incomplete.		X	19A - 3/31/2008 19B - 6/1/2008		Low

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-20	This is a component level finding. KPMG noted several access control weaknesses for the [redacted] solution during test work. Specifically, KPMG noted: - The [redacted] sever does not maintain information on user account creation and inactivity and therefore cannot terminate inactive accounts or provide audit information regarding the creation of [redacted] accounts, - Accounts that did not recertify during the recertification time period or were marked for deletion during the recertification period remained active on the system after the accounts should have been deactivated by [redacted] administrators, - Procedures for recertifying accounts were not fully implemented and accounts were recertified by means beyond those identified in documented procedures.	1.Automate the recertification process in order to remove the need for after-the-fact recertification via methods not documented in recertification procedures (email, verbal, etc.) 2.Configure the [redacted] servers to store information about the creation dates and activity of users in order to be able to properly identify inactive accounts and allow for their deletion. 3.Improve the process of deactivating accounts at the end of the recertification period and ensure that all accounts that should be removed from the system are removed.	CBP concurs with the finding. -CBP will research ways to improve and automate the current manual recertification process. The recertification procedures will be documented and updated as needed. -CBP will research solutions with vendors and network engineering to improve reporting modules and configurations to the [redacted] server to store and archive data about the users. Procedures for deactivating accounts at the end of the recertification process will be improved. -Pending an automated solution, the following mitigation is being pursued to improve the [redacted] recertification process by making improvements to the Access Request System.		X	20A - 4/30/2008 20B - 4/30/2008 20C - 4/30/2008		Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-21	This is a system level finding. KPMG noted that when changes to a user's access are performed in the log of these events is not regularly reviewed by personnel independent from those individuals who made the changes.	CBP formalize procedures for reviewing these access change logs and that review of these logs is implemented on a periodic basis as set forth in criteria.	CBP developed and approved the Security Audit Log Procedure (6-21-2007). The ISSO reviews the logs on a periodic basis (4-5 times per week) to determine potential security violations and notifies the of any anomalies detected. For , a process is in place, and reviews have begun. Schedules for reviews are being developed.		X		21A-1/15/2008 21B-1/25/2008	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-22	This is a component level finding. KPMG noted that documents identified in FY 2006 as not having documented approval or approval dates still lack these required approvals and approval or effective date. Specifically, KPMG noted that: - [redacted] – No approval for majority of fiscal year - Configuration Management Code Migration Procedures for [redacted] – No approval or effective date - Configuration Management Code Migration Procedures for [redacted] – No approval date or effective date - Production Management Team Procedures – No approval, no change history - [redacted] Operations: Standard Operating Procedures – No approval	CBP implement procedures in OIT divisions to perform a review of all documentation to update, consolidate and approve the documented procedures in use by operational personnel.	CBP concurs with the NFR. The [redacted] document cited in this NFR has been corrected and appropriate approval information obtained. The other documents cited in this NFR will be corrected and appropriate approval information obtained by September 30, 2007. CBP will promulgate established formal approval processes and requirements throughout the OIT Program Offices and Divisions by September 30, 2007.		X		10/4/2007	Low

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-23	3 out of 5 selected [redacted] Emergency Changes did not have post-implementation Executive Approval as required by the new OIT emergency change procedures.	CBP/OIT management consistently apply emergency change management post-implementation procedures to all [redacted] emergency changes. Furthermore, post-implementation procedures should be regularly reviewed and provide regular feedback to change administrators to determine any post-implementation steps that may have been missed due to the expeditious nature of emergency changes.	CBP concurs with the finding but does not agree to the recommendation. Emergency changes in [redacted] continue to be made according to OIT procedures that require executive management approval prior to implementation rather than after. Over the past six months, OIT has conducted a thorough review of its change management processes, including emergency changes. This review resulted in the new OIT Change Management Handbook (OIT CM 2.17), which became effective in August, 2007.	X			1/28/2008	Medium
CBP-IT-07-24	The [redacted] re-certification process has several weaknesses. Of the 45 selected ports, none had formally documented communication between the responsible DFO and OFO headquarters as directed by the FY 2006 memorandum put out by Office of Finance	1.Apply procedures outlined in the newly distributed memorandum from Office of Field Operations dated April 27, 2007 2.Consistently document results of re-certifications at the port level and maintain documentation	Transferred remediation to OF.		X	12/11/2008		Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-25	This is a system-level finding. KPMG noted that the [redacted] does not have an ISSO, but has been assigned an interim ISSO. KPMG noted that the interim ISSO is not formally documented as the [redacted] ISSO.	1.Formally document the appointment of the [redacted] Interim ISSO with a formal designation letter, and 2.Appoint a full time ISSO for the [redacted] and document that appointment with a formal designation letter.	CBP has appointed a full-time ISSO for the [redacted] to perform the duties stated in the designation letter in accordance with information technology security regulations and requirements. The audit recommended actions have been completed.	X			25A - 9/6/2007 25B - 9/6/2007	Low
CBP-IT-07-26	This is a system-level finding. KPMG noted that evidence of the review of these violation logs for 6 of 25 dates were not available for review.	CBP perform periodic review of access violation logs.	CBP has already developed and approved the [redacted] Log Procedure. The [redacted] is reviewing the access change logs on a periodic basis (4-5 times per week) to determine potential security violations. The reports of the access change logs will be retained by the [redacted] for a period of one year. In addition to immediately notifying the CSIRC of any confirmed security anomalies, the [redacted] will also provide to the ISSM a monthly report of all security anomalies identified and researched.	X			1/25/2008	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-27	This is a system-level finding. KPMG noted that authorizations are not being maintained for personnel that have administrator access to	1.Develop and implement procedures to restrict access to administrative capabilities, and 2.Require documented authorization requests and approval for each person requiring access to the mainframe administrative capabilities.	CBP concurs with this finding. In response to a related NFR (CBP-IT-07-16), CBP has already agreed to revise the applicable policy. With the revised policy, CBP will also develop new processes to control and document access for each individual requiring mainframe administrative capabilities. The target completion date for the policy revision was set as September 30, 2007. The target date for the new process and procedures is December 31, 2007.	X		27A-5/15/2008 27B-5/15/2008		High
CBP-IT-07-28	This is a system-level finding. KPMG noted that access policies and procedures have not been formally documented for the . KPMG also noted that access authorization forms were not completed for 27 out of 45 accounts created in FY 2007.	1.Develop and implement access policies and procedures for the to document formal methods for requesting and approving access for the 2.Require documented authorization requests and approval for each person requiring access to the	CBP will implement a that the Government Supervisor will fill out and sign to get a new or change an active account. The implementation of the form will be by September 15, 2007.	X			28A-10/25/2007 28B-10/25/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-29	This is a component-level finding. KPMG noted that procedures have been developed and a new termination form (CF-241) has been developed for use in terminating employees. KPMG notes that while these procedures address the submission of the form to System Security and require notification of removal of system access from System Security, the new procedures were developed and activated in June, 2007. The procedures are currently not implemented.	Implement the recently developed procedures for completion of the termination forms and notify System Security for all terminating employees so that systems access can be removed appropriately.	Transferred remediation to OF.		X	12/11/2008		Medium
CBP-IT-07-30	This is a system-level finding. KPMG noted that multiple terminated employees retained active accounts on the [redacted]. They were disabled as a result of accounts being inactive for 90 days. Therefore, these accounts were active 90 days after the employee terminated from US CBP.	1.Work with other US CBP Offices and within OIT to receive notice of termination of employees in a timely manner so that accounts can be deactivated on the departure of the employee. 2.Terminate accounts for terminated employees in a timely manner.	CBP concurs with this finding. The Office of Finance published a new directive for the Separation Procedures for Government Employees. The solution to this finding will require all CBP applications to interface with the [redacted] program in order to deactivate accounts automatically. Beginning in November 2007 OIT will begin coordinating with other CBP offices to develop a coordinated plan of action to address this finding	X		30A-4/15/2008 30B-4/15/2008		High

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-31	KPMG noted that 12 of the 45 selected ports/headquarters did not have self inspection worksheets completed. Accordingly, KPMG was not able to determine whether specific high risk combinations of roles were performed at these ports/headquarters	1.Apply procedures outlined in the newly distributed memorandum from Office of Field Operations 2.Consistently document results of re-certifications at the port level.	Transferred remediation to OF.		X	12/11/2008		Medium
CBP-IT-07-32	This is a new finding for FY 2007. KPMG selected 20 out of 201 changes and noted the following: - 9 of the 20 changes did not have formal test plans or documented results - None of the changes showed evidence of review of the documented test results	CBP management and ensure that all program offices appropriately document all test data, transactions, and program change results	Project teams will ensure that test documentation is attached to all change requests (Ascendant OMS of specific types), and the test documentation will record the reviewer's name as well as the review date. The Operational Maintenance Procedure will be edited accordingly, and enacted October 1st 2007.	X			12/5/2007	Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-33	This is a new finding for FY 2007. KPMG selected 15 of 90 changes and noted the following: - 3 of the 15 selected changes did not have formally documented test plans or test results. - None of the changes showed evidence of review of the test results documented.	CBP management and the OIT CCB ensure that all program offices appropriately document all test data, transactions, and program change results to monitor the quality of program changes.	CBP concurs with the finding. Management will take further steps to monitor the quality of changes to , including the review of test documentation and test results. The OIT CM 2.01 Policy dated June 12, 2006 has implemented the requirement that all project documentation be stored in the OIT Configuration Management (CM) tool, Dimensions. Also, Quality Assurance review will be completed to track metrics and recommend additional improvements to the process if needed.	X		3/14/2008		Medium

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-34	This is a component-level finding. KPMG noted that virus protection is not installed on all CBP workstations. Specifically, KPMG noted at the time of testing that approximately 6,000 of CBP's approximate 38,000 workstations do not have antivirus protection installed. Since the initial testing was performed, KPMG has noted that immediate remediation has begun and as of September 28, 2007 improvements have been made but 1,557 out of 42,429 workstations still are missing virus protection software.	CBP ensure that antivirus protection is installed on all workstations under the control of CBP.	CBP concurs with the finding and has already begun remediation activities. Only 1,557 out of 42,429 workstations are missing virus protection software. CBP will continue to utilize the reporting function of , which has the capability of searching for virus definition files that are more than 5 updates behind and to search for workstations that do not have the agent installed ("Uninstalled" status). A project is being undertaken by the DHS to ensure that rogue systems are identified and workstations that do not have the agent installed will be forced to do so. Also, with the new rollout of 4.0, the will require that any workstation authenticating to the domain will automatically have the agent installed. Estimated Completion: 12/31/2007	X		5/15/2008		High

NFR #	Condition	Recommendation	CBP Plans to Resolve	New Issue	Repeat Issue	Scheduled Completion Date	Actual Completion Date	Risk Rating
CBP-IT-07-35	During our technical testing, eighteen configuration management exceptions were identified on [redacted] Controllers and hosts supporting the [redacted] application. These vulnerabilities are listed in an enclosed table.	The recommendations are listed in an enclosed table	CBP concurs with the finding. Anticipated completion of the corrective action is Dec 31, 2007.		X		2/13/2008	High
CBP-IT-07-36	During our technical testing, thirty-seven patch management exceptions were identified [redacted] Controllers and hosts supporting the [redacted] application. These vulnerabilities are listed in an enclosed table.	The recommendations are listed in an enclosed table.	CBP concurs with the finding. Anticipated completion of the corrective action is Dec 31, 2007.		X		2/13/2008	High

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, CBP
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, CBP
Chief Information Officer, CBP
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
CBP 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.