Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2008 Customs and Border 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-09-59

April 2009

Office of Inspector General

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

Homeland Security

April 16, 2009

Preface

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

This report presents the information technology (IT) management letter for the FY 2008 Customs and Border Protection (CBP) balance statement audit as of September 30, 2008. 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-09-09, November 2008) 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 2008 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 4, 2008, and the conclusions expressed in it. We do not express opinions on CBP's financial statements or internal control or make conclusions on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust 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 4, 2008

Inspector General
U.S. Department of Homeland Security

Commissioner
U.S. Customs and Border Protection

Chief Information Officer
U.S. Customs and Border Protection

We have audited the consolidated balance sheets of the U.S. Department of Homeland Security's (DHS) Customs and Border Protection (CBP) as of September 30, 2008 and 2007, and 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 2008 audit, 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.

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 significant deficiency presented in our *Independent Auditors' Report*, dated November 15, 2008, and represent the separate restricted distribution report mentioned in that report.

The comments described herein have been discussed with the appropriate members of management 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 2008 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 (DHS) Customs and Border Protection (CBP) as of September 30, 2008 and 2007, and 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. 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 audit. 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* – Controls that limit and monitor access to powerful programs that operate computer hardware and secure applications supported by the system.
- *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 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

Financial IT systems security is essential to achieving effective, reliable reporting of financial and performance data. As a part of our engagement to perform the financial statement audit, we performed an evaluation of the general controls over significant CBP financial IT systems. Effective general controls are typically defined by the GAO's FISCAM, in six key control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. In addition to general controls, financial systems contain application controls, which are the structure, policies, and procedures that apply to use, operability, interface, edit and monitoring controls of an application. We tested various application controls of key CBP financial systems as part of our IT audit test work.

During fiscal year (FY) 2008, CBP took corrective action to address prior year IT control weaknesses. For example, CBP made improvements in how they track the hiring, termination and systems access of contracted employees within the Office of Information Technology (OIT). Also, issues with the tracking of backup tapes and their location were addressed, as well as issues surrounding the management review of control overrides performed in the However, during FY 2008, 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. 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 significant deficiency for CBP under standards established by the American Institute of Certified Public Accountants (AICPA). The information technology findings were combined into one significant deficiency regarding Information Technology for the FY 2008 audit of the CBP consolidated financial statements.

Although we noted improvement, many of the conditions identified at CBP in FY 2007 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 2008, CBP took steps to address these conditions. Despite these improvements, CBP needs further emphasis on the monitoring and enforcement of access controls. CBP needs to further emphasize the importance of developing and implementing well-documented procedures at the system and entity-level. Many of the issues identified during our review, which were also identified during FY 2007 and prior, can be addressed through a more consistent application of DHS and CBP policies for IT controls.

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

Conditions: In FY 2008, the following IT and financial system control weaknesses were identified at CBP. Many of the issues identified during our FY 2008 engagement were also identified during FY 2007. The following IT and financial system control weaknesses result in IT being reported as contributing to a significant deficiency for financial system security.

1. Access controls – we noted:

   - Some active connections to do not have documented interconnection security agreements (ISA) in place;

   - CBP does not maintain a centralized listing of contract personnel, including employment status. Currently, CBP only maintains contractor information for OIT contractors. While this is a majority of CBP contractors, it does not include all CBP contractors. Additionally, as a result of additional test work, we noted data validity issues in the ;

   - CBP workstation policy for screensavers is not appropriately implemented. Specifically we noted that the configuration of a password-protected screensaver can be modified by the user, allowing that user to remove the password requirement and also disabling the screensaver completely;

   - The following issues in regard to for the :
     - A solution has been implemented to track and monitor security and audit related activity but has not been operational for the entire fiscal year;
     - There is a configuration weakness for capturing security and audit related activity in the Protection application. The configuration has changed on multiple occurrences in regards to tracking activity for the ' to ' field in FY 2008; and
     - There is no defined method to generate and review security audit logs for security violations.

   - CBP implemented a script to disable accounts after thirty days of inactivity. However, the script was not functioning appropriately for most of the fiscal year and was only remedied during the third quarter of FY 2008;

   - A total of 10 mainframe audit logs were not available for the following dates: November 12, 2007, February 22, 2008, and March 7, 2008. For November 12, 2007, logs were not available for , and . For February 22, 2008, logs were not available for the and . For March 7, 2008, logs were not available for , and . It was further noted that all mainframe audit and system utility logs that went digital after April 1, 2008 were available for review;

   - has been adjusted to limit active temporary and/or emergency access to 24 hours after the request. It was noted, however, that the emergency table is still in use. Further, administrator or supervisory approval is not required each time temporary or emergency access is activated.

Also, Information System Security Manager (ISSM) approval is not required, conflicting with DHS policy;

- There are currently no procedures in place for the completion of semi-annual recertifications of the accounts. KPMG also notes that a recertification of the accounts is not performed on a semi-annual basis;

- 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 that initiated the changes. It was further noted that logs from March 2008 through July 2008 have not been reviewed by the Information System Security Officer (ISSO) or an independent reviewer;

- Out of 25 dates selected for review, six security violation report reviews were not available;

- Authorizations are not being maintained for personnel that have administrator access to the access control program. Additionally, it was noted in FY 2008 that access requests for new mainframe are requested and approved verbally;

- Access request forms were not available for review for three accounts created by the administrators during FY 2008;

- CBP-241 Employee Separation Forms are not completed consistently, with employee and/or supervisor signature missing from 7 of the 25 separated employees selected;

- Formal procedures do not exist for the security violation log review process. It was further noted that informal procedures are used by the network security specialist to inspect the security violation log for suspicious activity and to document the review;

- Formal procedures do not exist for the review process of audit and . It was further noted that informal procedures are used by the ISSOs to inspect logs for suspicious and unusual activity and to document the review;

- The special characters requirement under password complexity was not appropriately configured for

- Access authorizations for emergency and temporary access to are not approved by the ISSM, as required by DHS policy;

- A Customs Directive was provided as separation procedures for contractors and this directive was dated September 2001. The directive references Treasury policies as source documentation. This directive is out of date, as CBP is no longer a part of the Department of Treasury. Additionally, CBP-242 contractor separation forms are not completed consistently for separating CBP contractors. Specifically, it was noted that all forms for selected separated contractors were completed; however, 6 of the selected 25 separated contractors' forms were completed at least one month after the individual separated from CBP;

- Non-disclosure agreements (NDAs) are not consistently mandated for CBP contractors;

- The parameters for the audit and ( ) are not configured to collect appropriate data. KPMG further noted that three out of the six do not produce any data in the log;

- CBP does not currently require individuals to sign a rules of behavior prior to gaining access to CBP information systems;

- The following weaknesses were identified for the Security Audit Logs procedures:
  - Procedures do not define how often the security audit logs are reviewed.
  - Procedures do not describe the documented evidence of review process, Security Violation Log Report, which is created by the ISSO/Independent Reviewer.
  - Procedures do not define the sampling methodology that is used to select daily security logs.
  - Procedures were not effective for all of FY 2008 (October 1, 2007 – September 30, 2008);

- The initial password granted to new accounts is not in compliance with DHS requirements;

- CBP does not have a method of tracking completion of security awareness training for CBP employees and contractors. Individuals from the program team responsible for security awareness training do not have the ability to identify those individuals who have not completed security awareness training and, therefore, can not ensure all CBP personnel have completed this training;

- The Security Administrators Handbook is out of date and has inaccurate statements of CBP and DHS policies. Specifically, the following weaknesses were identified:
  - Out-of-date references to US Customs Service,
  - References to out-of-date Customs (now CBP) policies and procedures (1400-05a),
  - Requirement that initial passwords are set to a weak password string,
  - Statement that does not allow special characters in passwords;

- The following weaknesses were identified in access control procedures:
  - A periodic (at least semi-annual) recertification of all portal accounts is not performed,
  - Formal procedures are not documented for the creation of portal accounts,
  - is not configured to disable accounts after 45 days of inactivity on the system; and

- Two accounts that were created during FY 2008 did not have appropriate access authorization forms maintained by the administrators. It was further noted that multiple administrators on the had accounts created by other groups than the Support Team.

2. Application software development and change controls – no condition noted.

3. Service continuity – we noted:

   - is not installed on all workstations for the majority of the fiscal year as required. Specifically, it was noted that as of 3/31/2008, 4,751 workstations out of 50,282 workstations do not have installed;
   - That a complete and up-to-date listing of all CBP workstations is not maintained;
   - the system used to enforce virus protection policies, was not installed on all CBP workstations on . It was noted that as of 8/11/2008, 0.25% of all workstations on did not appear on the listing. In addition to this, a conclusion could not be obtained on whether all CBP workstations have antivirus protection, as those workstations that are not on are not communicating with ;
   - The most recent business continuity planning (BCP) testing was incomplete. Specifically, it was noted that not all systems were brought online as required since sufficient hardware was unavailable at the recovery facility to fully and properly perform the continuity testing; and
   - Documented hardware maintenance procedures do not exist for the environment supporting .

4. Entity-wide security program planning and management – no conditions noted.

5. System software – we noted during our technical testing:

   - Configuration management exceptions were identified on and hosts supporting the and applications; and
   - Patch management exceptions were identified on hosts supporting the and the applications.

6. Segregation of duties – no conditions noted.

Recommendations: We recommend that the CBP Office of Chief Information Officer (OCIO), in coordination with the Office of the Chief Financial Officer (OCFO), make the following improvements to the CBP financial management systems:

1. For access controls:

   - Review and maintain a listing of active connections with the and account for each connection with a documented interconnection security agreement (ISA);

- Work on the to ensure that all CBP contractors are included in the database and that the data for each contractor is complete and accurate;

- Determine a method for appropriately applying CBP and DHS policy requiring automatically-activated, password-protected screensavers after a period of inactivity;

- Properly capture appropriate audit log data per DHS policy. KPMG further recommends that a method for generating and reviewing security audit logs be developed for the according to CBP and DHS policy, to detect potential security events;

- Regularly run the updated script on the system to disable user accounts after the DHS-specified period of inactivity;

- Maintain audit and per DHS policy;

- Develop and implement procedures that will appropriately restrict the use of emergency or temporary access within and that requires documented supervisory approval from the ISSM confirming this access is needed. In addition, CBP should perform regular recertifications of the emergency access table to ensure persons with the capability to request temporary or emergency access need to remain on the emergency access table;

- Develop formal procedures for recertifying accounts and access to shared data and perform regular recertifications of accounts and access to shared data as required by developed procedures;

- Implement the review of security audit logs on a periodic basis by an independent reviewer and formalize these procedures in detail for the review of security audit logs;

- Follow DHS policy and maintain documented evidence of review for security violation logs for the duration outlined in DHS policy;

- Develop and implement procedures to restrict access to mainframe administrative capabilities and require documented authorization requests and approval for each person requiring access to the administrative capabilities;

- Continue to develop a method for tracking and consolidating access request forms for the and continue to implement the procedures developed to control account creation;

- Require managers to consistently complete the CBP-241 forms that are required as set forth in CBP directives and policy;

- Create formal procedures to document the security violation log review process;

- Create formal procedures to document the review process for audit and ;

- Follow DHS policy and improve password complexity by including special characters for the application;

- Adjust CBP-level and -level policies to require the ISSM to approve the emergency and temporary access authorizations prior to access being granted. Require documented supervisory approval from the ISSM each time a user requires emergency access abilities;

- Review contractor separation directives, document an up-to-date review of this document and make modifications as needed based on the new operating environment for CBP as part of the Department of Homeland Security. Require the consistent and accurate completion of the CBP-242 forms for all separating contractors;

- Enforce DHS' requirement that a non-disclosure agreement be signed by all contractors in a moderate and high risk level position to ensure that they are aware of their responsibilities in protecting the confidentiality of DHS and CBP data;

- Properly configure audit and to capture appropriate data for the and that CBP maintain audit and per DHS policy;

- Require all employees and contractors sign rules of behavior prior to being granted any system access. Additionally, for personnel that already have systems access, CBP should prioritize having these individuals sign rules of behavior to maintain their systems access;

- Create detailed procedures that document the review process for security audit logs that includes the documented evidence of review;

- Update the Security Administrator Handbook to require a strong password that is in compliance with DHS and CBP password policies to be set as the initial password for all new accounts;

- Develop a method for determining individuals who have and have not completed security awareness so that they can actively work towards 100% compliance with the DHS requirement that all individuals with systems access complete annual security awareness training;

- Perform a full review of the Security Administrators Handbook and updates be made to the document to reflect the current operating environment. This review should be fully documented and the Handbook should be updated to include a change log as evidence of the updates made;

- Document and implement policies and procedures for access control; and

- Limit the organization that can create accounts and administrator accounts and require any accounts created to be created by a single organization.

2. No findings or recommendations were noted for application software development and change control.

3. For service continuity:

- Implement procedures to regularly review and monitor the workstations that have installed and perform inquiries to determine why identified workstations do not have installed;
- Work with administrators across the country to ensure that new and existing workstations are added to a CBP domain to appropriately account for all workstations;
- Develop procedures to regularly review and monitor the workstations that have antivirus protection installed and perform inquiries to determine why identified workstations do not have the protection installed and updated;
- Work to allocate the appropriate hardware at to allow for the system availability to fully test the business continuity plan to ensure that has the capability to support CBP in the event that the is rendered unavailable for production; and
- Document hardware maintenance procedures to ensure a consistent application of maintenance methodologies for the environment.

4. No findings or recommendations were noted for entity-wide security program planning and management.

5. For system software:
   - Immediately address configuration management exceptions that were identified during technical testing on) and hosts supporting the and applications; and
   - Immediately address patch management exceptions that were identified during technical testing on hosts supporting the and the and applications.

6. No findings or recommendations were noted for segregation of duties.

Cause/Effect: Due to the increased allocation of resources to the development and implementation project, organizational realignments, and staff turnover, resources were not consistently available throughout the year to address all prior year issues noted above. While CBP addressed a significant number of prior year issues, several remain unresolved. Some issues from the prior year have already been addressed; however, the findings were reissued as these findings were not resolved for the entire fiscal year, which is within the scope of the audit. Additionally, several weaknesses were noted as a result of changes in DHS policy since FY 2007 that had not been incorporated into CBP policy and implementation. By not addressing the conditions noted above, the possibility exists for CBP that these risks will be exploited, in either a singular fashion or in combination which might affect the availability, confidentiality or integrity of CBP's financial data.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition, OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. In closing, for this year's IT audit, we assessed CBP's compliance with *DHS 4300A Sensitive Systems Handbook*. Additionally, we assessed CBP's implementation of CBP policy, the *Information Systems Security Policies and Procedures Handbook, version 1.3*.

APPLICATION CONTROL FINDINGS

During FY 2007, KPMG noted that weaknesses over the processing of drawback claims exist within the system. Specifically, did not support the tracking of drawback items to the line item level. Rather, only tracked 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 a significant control weakness and also noted by the KPMG IT team.

Also, due to the design of , certain controls could 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. did not generate override reports for supervisory review.

In FY 2008, KPMG noted that CBP OIT had developed a report in which displays all control overrides performed at a particular port within . KPMG determined that the report appropriately accounts for all overrides in order to address the condition identified in previous fiscal years and identified above. Due to the pervasiveness of this application control weakness, the mitigating control only partially alleviates the control weakness through implementing this report review process. Therefore, this issue remains a material weakness specific to drawbacks when combined with the resulting financial audit test work. This material weakness for drawbacks is reported in our *Independent Auditors' Report*, dated November 15, 2008.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the CBP CIO. Generally, CBP management agreed with all of our findings and recommendations and they have developed a remediation plan to address these findings and recommendations. We have incorporated these comments where appropriate an included a copy of the comments in Appendix D. We have corrected the risk rating assigned to the notice of findings and recommendation within this report. The risk rating now corresponds with the risk rating presented in the FY 2008 Consolidated Information Technology Management Letter.

OIG Response

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

APPENDIX A

DESCRIPTION OF KEY FINANCIAL SYSTEMS AND IT INFRASTRUCTURE WITHIN THE SCOPE OF THE FY 2008 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 2008 Financial Statement Audit.

Locations of Review:

The in .

The in .

The in .

The Port of .

The Port of .

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 using a phased approach that replaced the - based financial system.

- – is a collection of business process mainframe-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.

- – is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. is being deployed in phases, with a final full deployment scheduled for FY 2012. As is partially implemented now and processes a significant amount of revenue for CBP, was included in a limited scope in the FY 2008 financial statement audit.

- – Used for tracking seized assets, Customs Forfeiture Fund, and fines and penalties. The resulting financial information interfaces with CBPs financial management system.

APPENDIX B

FY 2008 NOTICES OF IT FINDINGS AND RECOMMENDATIONS

Notice of Findings and Recommendation – Definition of Risk Ratings:

The Notice of Findings and Recommendations (NFR) are ranked with a risk rating of High, Medium, and Low based upon the potential impact that each weakness could have on CBP's information technology (IT) general control environment and the integrity of the financial data residing on the CBP's financial systems, and the pervasiveness of the weakness. The risk ratings are intended only to assist management in prioritizing corrective actions, considering the potential benefit of the corrective action to strengthen the IT general control environment and/or the integrity of the CBP financial statements. Correction of some higher risk findings may help mitigate the severity of lower risk findings, and possibly function as a compensating control. In addition, analysis was conducted collectively on all 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. The risk ratings, used in this context, are not defined by *Government Auditing Standards*, issued by the Comptroller General of the United States, or the American Institute of Certified Public Accountants (AICPA) Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Standards and reported in our *Independent Auditors' Report* on the CBP's financial statements, dated December 4, 2008.

High Risk: A control weakness that is more serious in nature affecting a broader range of financial IT systems, or having a more significant impact on the IT general control environment and /or the integrity of the financial statements as a whole.

Medium Risk: A control weakness that is less severe in nature, but in conjunction with other IT general control weaknesses identified, may have a significant impact on the IT general control environment and / or the integrity of the financial statements as a whole.

Low Risk: A control weakness minimal in impact to the IT general control environment and / or the integrity of the financial statements.

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

U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2008

U.S. Customs and Border Protection
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-02	This is a system-level finding. KPMG notes that significant progress has been made at addressing this persistent finding. KPMG notes that a full listing of connections to has been developed and is maintained. However, KPMG also noted that there are active connections to that still do not have a documented in place. Work is progressing within CBP to address the missing but as of testing, KPMG noted that not all connections had a documented .	KPMG believes that work should continue to review and maintain a listing of active connections with the and account for each connection with a documented .		*X*	**Medium**
CBP-IT-08-03	This is a repeat, component-level finding. CBP does not maintain a centralized listing of contract personnel, including employment status. Currently, CBP only maintains contractor information for OIT contractors. While this is a majority of CBP contractors, it does not include all CBP contractors. Additionally, as a result of additional test work, KPMG noted data validity issues in the .	KPMG recommends that CBP continue work on the to ensure that all CBP contractors are included in the database and that the data for each contractor is complete and accurate.		*X*	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-08	This is a system-level finding. KPMG noted the following issues in regards to Security Audit Logs for : • A solution has been implemented to track and monitor security and audit related activity but has not been operational for the entire FY 2008. • There is a configuration weakness for capturing security and audit related activity in the application. The configuration has changed on multiple occurrences in regards to tracking activity for the 'Logon to Account' field in FY 2008. • There is no defined method to generate and review security audit logs for security violations for the .	Properly configure the application to capture appropriate data per DHS policy. KPMG further recommends that a method for generating and reviewing security audit logs be developed for according to CBP and DHS policy, to detect potential security events.		*X*	**Low**
CBP-IT-08-09	This is a system-level finding. KPMG noted that during FY 2008, CBP implemented a script to disable accounts after thirty days of inactivity. However, KPMG noted that the script was not functioning appropriately for the full fiscal year and was fixed during the third quarter of FY 2008.	Ensure that the updated script runs regularly on the system to disable user accounts after the DHS-specified period of inactivity.		*X*	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-12	This is a component-level finding. As noted in FY 2007, KPMG notes that [redacted] is not installed on all workstations for the majority of the fiscal year. Specifically, KPMG noted that as of 3/31/2008, 4,751 workstations out of 50,282 accounted for workstations do not have [redacted] installed.	Develop procedures to regularly review and monitor the workstations that have [redacted] installed and perform inquiries to determine why identified workstations do not have [redacted] installed.		***X***	**Medium**
CBP-IT-08-13	This is a component-level finding. KPMG noted that while progress has been made in accounting for all CBP workstations, a complete and up-to-date listing of all CBP workstations is not maintained.	Work with administrators across the country to ensure that new and existing workstations are added to a CBP [redacted] domain to allow for all workstations to be accounted for in an appropriate fashion.		***X***	**Medium**
CBP-IT-08-16	This is a system-level finding. KPMG noted that the [redacted] has been adjusted to limit active temporary and/or emergency access to 24 hours after the request. KPMG notes, however, that the table is still being used and that administrator or supervisory approval is not required each time temporary or emergency access is activated and that ISSM approval is not required, as required in DHS policy.	a) Develop and implement procedures that will appropriately restrict the use of emergency or temporary access within [redacted] and that requires documented supervisory approval from the ISSM confirming this access is needed. b) Perform regular recertifications of the emergency access table to ensure persons with the capability to request temporary or emergency access need to remain on the emergency access table.		***X***	**Medium**
CBP-IT-08-18	This is a system-level finding. KPMG noted there are currently no procedures in place for the completion of semi-annual recertifications of [redacted] accounts. KPMG also notes that a recertification of [redacted] accounts is not performed on a semi-annual basis.	a) Develop formal procedures for recertifying [redacted] accounts and access to shared data. b) Perform regular recertifications of [redacted] accounts and access to shared data as required by developed procedures.		***X***	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-21	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 that made the changes. KPMG further noted that logs from March 2008 through July 2008 have not been reviewed by the ISSO/Independent Reviewer.	Implement the review of these logs on a periodic basis by an independent reviewer and that CBP formalize these procedures in detail for the review of security audit logs.		***X***	**Low**
CBP-IT-08-26	This is a system-level finding. KPMG noted that out of 25 dates, security violation report reviews were not provided to KPMG.	Follow DHS policy and maintain documented evidence of review for security violation logs for the duration outlined in DHS policy.		***X***	**Low**
CBP-IT-08-27	This is a system-level finding. KPMG noted that authorizations are not being maintained for personnel that have administrator access to . Additionally, KPMG noted in FY 2008 that access requests for new mainframe administrator accounts are requested and approved verbally.	a) Develop and implement procedures to restrict access to administrative capabilities, and b) Require documented authorization requests and approval for each person requiring access to the administrative capabilities.		***X***	**Medium**
CBP-IT-08-28	This is a system level finding. KPMG noted that procedures have been developed to require access request forms for any new account created for the . However, KPMG noted that access request forms were not available for review for three accounts created by administrators during FY 2008.	Continue efforts to develop a method for tracking and consolidating access request forms for the and continue to implement the procedures developed to control account creation.		***X***	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-29	This is a component-level finding. KPMG noted that procedures are in place for the completion of the termination forms for separating government employees. KPMG noted, however, that the forms are not completed consistently, with employee and/or supervisor signature missing from 7 of the 25 separated employees selected.	Require managers to consistently complete the CBP-241 forms that are required as set forth in CBP directives and policy.		*X*	**Medium**
CBP-IT-08-34	This is a component-level finding. KPMG noted that , the system used to enforce virus protection policies, was not installed on all CBP workstations on . KPMG noted that as of 8/11/2008, 0.25% of all workstations on did not appear on the listing. In addition to this, KPMG could not conclude on whether all CBP workstations have antivirus protection, as those workstations that are not on are not communicating with	Develop procedures to regularly review and monitor the workstations that have antivirus protection installed and perform inquiries to determine why identified workstations do not have the protection installed and updated.		*X*	**Low**
CBP-IT-08-35	During our technical testing, configuration management exceptions were identified on and hosts supporting the and applications.	Immediately address configuration management exceptions that were identified during technical testing on Controllers and hosts supporting the and applications.		*X*	**High**
CBP-IT-08-36	During our technical testing, patch management exceptions were identified on hosts supporting the and the and applications.	Immediately address patch management exceptions that were identified during technical testing on hosts supporting the and the and applications.		*X*	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-37	This is a system-level finding. KPMG noted that formal procedures do not exist for the security violation log review process. KPMG further noted that informal procedures are used by the network security specialist to inspect the security violation log for suspicious activity and to document the review.	Develop formal procedures to document the security violation review process.	*X*		**Low**
CBP-IT-08-38	This is a system-level finding. KPMG noted that formal procedures do not exist for the review process of audit and . KPMG further noted that informal procedures are used by the ISSOs to inspect logs for suspicious and unusual activity and to document the review.	Develop formal procedures to document the review process for audit and .	*X*		**Low**
CBP-IT-08-39	This is a system-level finding. KPMG noted that the 'special characters' requirement under password complexity is not set.	Follow DHS policy and improve password complexity by including special characters for the application.	*X*		**Low**
CBP-IT-08-40	This is a system-level finding. KPMG noted that access authorizations for emergency and temporary access to are not approved by the ISSM.	a) Adjust CBP-level and -level policies to require the ISSM to approve the emergency and temporary access authorizations prior to access being granted, and b) Require documented supervisory approval from the ISSM each time a user requires emergency access abilities.	*X*		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-41	This is a component-level finding. KPMG noted that a Customs Directive was provided as separation procedures for contractors and the directive was dated September 2001. The directive references Treasury policies as source documentation. This directive is out of date as CBP is no longer a part of the Department of Treasury. Additionally, KPMG noted that CBP-242 contractor separation forms are not completed consistently for separating CBP contractors. Specifically, KPMG noted that all forms for selected separated contractors were completed; however, 6 of the selected 25 separated contractors' forms were completed at least one month after the individual separated from CBP.	a) Review the current directive, document an up-to-date review of this document and make modifications as needed based on the new operating environment for CBP as part of the Department of Homeland Security, and b) Require the consistent and accurate completion of the CBP-242 forms for all separating contractors.	*X*		**Medium**
CBP-IT-08-43	This is a component-level finding. KPMG noted that the most recent business continuity plan testing was incomplete. Specifically, KPMG noted that not all systems were brought online as required since sufficient hardware was unavailable at the recovery facility to fully and properly perform the continuity testing.	Allocate the appropriate hardware to to allow for the system availability to fully test the business continuity plan to ensure that has the capability to support CBP in the event that the is rendered unavailable for production.	*X*		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-44	This is a component-level finding. KPMG noted that non-disclosure agreements (NDAs) are not consistently mandated for CBP contractors.	Enforce DHS' requirement that a non-disclosure agreement be signed by all contractors in a moderate and high risk level position to ensure that they are aware of their responsibilities in protecting the confidentiality of DHS and CBP data.	*X*		**Low**
CBP-IT-08-45	This is a system-level finding. KPMG noted that the parameters for the [redacted] are not configured to collect appropriate data. KPMG further noted that three out of the [redacted] audit and system utility logs, [redacted], do not produce any data in the log.	Properly configure [redacted] audit and [redacted] to capture appropriate data for the [redacted] system.	*X*		**Low**
CBP-IT-08-46	This is a system-level finding. KPMG noted that a total of 10 specific logs were not available for the following dates: November 12, 2007, February 22, 2008, and March 7, 2008. For November 12, 2007 logs were not available for [redacted]. For February 22, 2008, logs were not available for the [redacted], and [redacted]. For March 7, 2008, logs were not available for [redacted] KPMG further noted that all mainframe audit and system utility logs that went digital after April 1, 2008 were available for review.	Maintain [redacted] audit and system utility logs per DHS policy.	*X*		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-47	This is a component-level finding. KPMG noted that CBP does not currently require individuals to sign rules of behavior prior to gaining access to CBP information systems.	Require all CBP personnel (employees and contractors) sign rules of behavior prior to being granted any system access. Additionally, for personnel that already have systems access, CBP should prioritize having these individuals sign rules of behavior to maintain their systems access.	*X*		**Low**
CBP-IT-08-48	This is a system level finding. KPMG noted the following weaknesses for the Security Audit Logs procedures below: • Procedures do not define how often the security audit logs are reviewed, • Procedures do not describe the documented evidence of review process, Report that is created by the ACS ISSO/Independent Reviewer, • Procedures do not define the sampling methodology that is used to select daily security logs, and • Procedures were not effective for the entire FY 2008 (October 1, 2007 – September 30, 2008).	Develop detailed procedures that document the review process for security audit logs that includes the documented evidence of review.	*X*		**Low**
CBP-IT-08-49	This is a system-level finding. KPMG noted that the initial password granted to new accounts is not in compliance with DHS requirements.	Update the Security Administrator Handbook to require a strong password that is in compliance with DHS and CBP password policies to be set as the initial password for all new accounts.	*X*		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-50	This is a component-level finding. CBP has no method of tracking completion of security awareness training for CBP employees and contractors. Individuals from the program team responsible for security awareness training do not have the ability to identify those individuals who have not completed security awareness training. Therefore, CBP can not ensure all personnel have completed this training.	Develop a method for determining individuals who have and have not completed security awareness so that they can actively work towards 100% compliance with the DHS requirement that all individuals with systems access complete annual security awareness training.	*X*		**Low**
CBP-IT-08-51	This is a system level finding. KPMG noted through inquiry with the that documented hardware maintenance procedures do not exist.	Document hardware maintenance procedures to ensure a consistent application of maintenance methodologies for the UNIX environment.	*X*		**Low**
CBP-IT-08-52	This is a system-level finding. KPMG determined that the CBP workstation policy for screensavers is not appropriately implemented. Specifically, KPMG noted that the configuration of a password-protected screensaver can be modified by the user, allowing that user to remove the password requirement and disable the screensaver completely.	Determine a method for appropriately applying CBP and DHS policy requiring automatically-activated, password-protected screensavers after a period of inactivity.	*X*		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-53	This is a system-level finding. The [redacted] Security Administrators Handbook is out of date and has inaccurate statements of CBP and DHS policies. Specifically, KPMG noted: • Out-of-date references to US Customs Service, • References to out-of-date Customs (now CBP) policies and procedures (1400-05a), • Requirement that [redacted] initial passwords are set to a weak password string, and • Statement that [redacted] does not allow special characters in passwords.	Perform a full review of the [redacted] Security Administrators Handbook and update the document to reflect the current operating environment. This review should be fully documented and the Handbook should be updated to include a change log as evidence of the updates made.	*X*		**Low**
CBP-IT-08-54	This is a system level finding. KPMG noted the following weaknesses in [redacted] access control procedures: • A regular (at least semi-annual) recertification of all [redacted] portal accounts is not performed, • Formal procedures are not documented for the creation of [redacted] portal accounts, and • [redacted] is not configured to disable accounts after 45 days of inactivity on the system.	Document and implement policies and procedures for [redacted] access control.	*X*		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-55	This is a system level finding. KPMG noted that 2 accounts created during FY 2008 did not have appropriate access authorization forms maintained by the administrators. KPMG further noted that multiple administrators on the had accounts created by other groups than the Support Team.	Limit the organization that can create accounts, administrator accounts and require any accounts be created by a single organization.	*X*		**Medium**

APPENDIX C

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

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-07-01	Override of warning in Drawback function without supervisory approval	**X**	
CBP-IT-07-02	Interconnection Security Agreements (ISAs)		CBP-IT-08-02
CBP-IT-07-03	Contractor Tracking Deficiencies		CBP-IT-08-03
CBP-IT-07-04	Labeling of Backup Media	**X**	
CBP-IT-07-05	Password Configurations	**X**	
CBP-IT-07-06	Session Disconnects and Locking	**X**	
CBP-IT-07-07	Version Control for Source Code	**X**	
CBP-IT-07-08	Audit Logs		CBP-IT-08-08
CBP-IT-07-09	Disabling of Inactive Accounts on		CBP-IT-08-09
CBP-IT-07-10	Physical Access Recertification	**X**	
CBP-IT-07-11			CBP-IT-08-46
CBP-IT-07-12	Install		CBP-IT-08-12
CBP-IT-07-13	Complete List of CBP Workstations		CBP-IT-08-13
CBP-IT-07-14	Backup Tape Withdrawal Logging	**X**	
CBP-IT-07-15	Inactive Accounts	**X**	
CBP-IT-07-16	Excessive Emergency Access		CBP-IT-08-16
CBP-IT-07-17	Review of	**X**	
CBP-IT-07-18	Recertification of Accounts		CBP-IT-08-18
CBP-IT-07-19	Security Awareness Training	**X**	
CBP-IT-07-20	Access Controls	**X**	
CBP-IT-07-21	Review of Changes to Security Profiles in		CBP-IT-08-21
CBP-IT-07-22	OIT Documentation Not Formally Approved	**X**	

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-07-23	Emergency Change Executive Approvals for	**X**	
CBP-IT-07-24	Re-recertification Process	**X**	
CBP-IT-07-25	No formal designation of ISSO for	**X**	
CBP-IT-07-26	Review of Security Violation Logs		CBP-IT-08-26
CBP-IT-07-27	Administrator Access Authorization Weaknesses		CBP-IT-08-27
CBP-IT-07-28	Access Policies and Procedures		CBP-IT-08-28
CBP-IT-07-29	Completion of CF-241 Forms for Terminated Employees		CBP-IT-08-29
CBP-IT-07-30	Removal of Terminated Employees from	**X**	
CBP-IT-07-31	High Risk Combinations	**X**	
CBP-IT-07-32	Change Documentation	**X**	
CBP-IT-07-33	Change Documentation	**X**	
CBP-IT-07-34	Installation of Anti-Virus Protection		CBP-IT-08-34
CBP-IT-07-35	Configuration Management		CBP-IT-08-35
CBP-IT-07-36	Patch Management		CBP-IT-08-36

FY 2007 Issued NFRs	FY2007 Closed NFRs	FY2007 Reissued NFRs
36	19	17

APPENDIX D

MANAGEMENT RESPONSE TO DRAFT U.S. CUSTOMS AND BORDER PROTECTION

IT MANAGEMENT LETTER

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

U.S. Customs and Border Protection

MAR 4 2009

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Charles Armstrong
Assistant Commissioner
Office of Information and Technology

SUBJECT: Draft Audit Report - Information Technology Management Letter for the Fiscal Year 2008 U.S. Customs and Border Protection Financial Statement Audit

This is in reply to your memorandum dated February 13, 2009, requesting written comments on the draft report and responses to the recommendations that are included in the subject Information Technology (IT) Management letter. The U.S. Customs and Border Protection (CBP) Office of Information and Technology (OIT) would like to provide the following comments on the remediation actions that are being performed for the findings and recommendations from the Fiscal Year (FY) 2008 audit.

General Comments

We note that last year the management letter was addressed to the Commissioner of CBP.

In addressing this year's letter directly to CBP OIT it was incorrectly addressed to the "Acting" Assistant Commissioner.

Concerning the risk level assigned to several of the findings, there are differences between this draft and the draft of the consolidated FY 2008 Department of Homeland Security Draft IT Management Letter which we reviewed last week. We request clarification on which risk levels are assessed for each finding.

Access Controls

CBP concurred with KPMG's recommendations in this area. All recommendations concerning the have been implemented. In addition, the recommendation dealing with IT Security Awareness training has been completed. Building on the the issues dealing with contractor access have also been addressed. The work on some issues

dealing with access and with the is still in progress. Corrective Action Plans (CAPs) have been implemented for the Notices of Findings and Recommendations (NFRs) and their status is provided in the attachment.

Service Continuity

CBP concurred with KPMG's recommendations in this area. The recommendation concerning maintenance of the environment has been completed. The recommendations concerning a complete count of workstations, , and ePolicy Orchestrator were closely related and interdependent. They are scheduled to be completed at the end of February, 2009. In regard to business continuity planning, the equipment is expected to be in place by July of this year.

System Software

CBP concurred with the KPMG recommendations in this area. CAPs have been implemented for the NFRs and their status is provided in the attached document.

Application Control

As noted by the auditors, CBP OIT developed a report in to account for all drawback overrides. This capability has been provided to users as a mitigation pending the future replacement of .

Thirty-four NFRs were issued to CBP OIT during the FY 2008 audit (15 were reissues of FY 2007 findings and 18 were new). To date, 14 have been completed and await closure, pending KPMG review. CAPs are in progress for the remaining recommendations and their status is provided in the attached.

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

Attachment

Status of Corrective Action Plans for FY 2008 Financial Audit NFRs issued to CBP OIT

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-02	**Interconnection Security Agreements**	**Weakness:** Without approved interconnection security agreements (ISA) for all system interconnections, connecting entities could compromise data and system integrity and create security vulnerabilities and risks for US Customs and Border Protection (CBP). **Recommendation:** CBP ensure that each active connection with should be accounted for and have documented ISAs.	CBP will continue to verify the number of entities that connect to . For those connections that do not have documented ISA agreements, ISAs will be created and reviewed by the Office of Information and Technology and the Security and Technology Policy Branch allowing for an accurate list of all entities that connect to .	On Track-Completion Date 6/15/09

[1] For the 2008 audit, OIG/KPMG Auditors used the following numbering system for NFRs: Repeat NFRs were assigned the same numbers used last year. NFRs numbered 1 through 36 are repeats and any skipped numbers were not reissued in 2008. NFRs numbered 37 and higher are new in 2008.

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High *however Consolidated statement said Medium*	CBP-IT-08-03	**Listing of Employed and Terminated Contractors**	**Weakness:** By not maintaining an updated and timely list of US Customs and Border Protection (CBP) contractors, risks are created concerning access to the financial systems, especially when the contractor leaves CBP. **Recommendation:** CBP ensure that the remains updated and includes all contractors. Also, all information regarding contractors is accurate and complete.	The has been developed and populated with data on contractors supporting CBP. Building passes are only being issued if the data on the contractor is in the system. A directive has been developed finalized and implemented requiring all CBP offices to enter the data on their contractors.	Completed-11/12/08
Medium *however Consolidated statement said Low*	CBP-IT-08-08	**Completion and Review of Security Audit Logs for**	**Weakness:** Without correct configuration of the application to capture appropriate data and the ability to review security audit logs, potential security violations may go undetected. **Recommendation:** CBP properly configure the application to capture appropriate data and a process for generating and reviewing security audit logs to be developed for that will detect potential security events.	CBP has ensured that the configuration change process implemented within the application and configuration changes have been completed to capture all security events. CBP implemented a process that ensures the effective automated audit log process to review security logs in order to detect potential security events.	Completed-10/01/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Low	CBP-IT-08-09	**Accounts are Not Disabled After an Appropriate Period of Time for the**	**Weakness:** Inactive accounts that are not suspended in a timely manner increase the risk that any individual may inappropriately access CBP systems. **Recommendation:** CBP ensure updated scripts runs regularly on the system to disable user accounts after the DHS-specified period of inactivity.	CBP updated the script to include all users accounts within the . Corrected script was executed on schedule and results confirmed.	Completed-10/15/08
Medium	CBP-IT-08-12	**Installation of on CBP Workstations**	**Weakness:** Without installed on workstations, there is no reasonable assurance that patched and security fixes are being appropriately applied to all CBP workstations. **Recommendation:** CBP develop procedures to regularly review and monitor the workstations that have installed and perform inquiries to determine why identified workstations do not have installed.	CBP is working to ensure that new and existing workstations are added to the CBP domain to allow all workstations to be accounted for and updated. CBP will also implement a process to ensure that is on all workstations.	On Track-Completion Date 2/28/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-13	**Incomplete Listing of CBP Workstations**	**Weakness:** Without the assurance of a list that includes all workstations connecting to CBP networks, CBP does not have the confidence that security patches and updates are being appropriately applies to all CBP workstations. This could lead to vulnerabilities be exploited and also lacks the ability to ensure group policies are implemented on all workstations. **Recommendation:** CBP work with administrators across the country to ensure that new and existing workstations are added to a CBP domain to allow for all workstations to be accounted for.	CBP is working to ensure that new and existing workstations are added to the CBP domain which will allow all workstations to be accounted for and updated. CBP is implementing a process to ensure that are on all workstations.	On Track-Completion Date 2/28/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High *however Consolidated statement said Medium*	CBP-IT-08-16	**Excessive Emergency and Temporary Access in**	**Weakness:** Without consistent emergency access authorization procedures, excessive emergency access to sensitive data operations with may exist. Without proper authorization each time a user requires emergency access, the user could gain access to data that they do not need and may be able to compromise the integrity of the data and disrupt processing. **Recommendation:** A. CBP develop and implement procedures that will appropriately restrict the use of emergency and temporary access within and that requires documented supervisory approval from Information Systems Security Manager (ISSM) confirming this access is needed. B. CBP perform regular recertifications of the emergency access table and ensure only certain users are included on the table and have the capability to request emergency access.	CBP has notified the programs that the CISO must approve list of supervisors who can approve emergency access as well as approving the current list of individuals with access and their profiles. For all CFO Designated Financial Systems the CISO was provided lists of all emergency access profiles, all developers who have emergency access, and all supervisors authorized to approve emergency access. The CISO sent out delegation letters to the owners of the financial systems delegating authority to specific supervisors so they can approve emergency access requests for all CFO Designated Financial Systems for 24 hours at a time, no more than 4 times a month per person, for one year. The CISO will re-certify the list of authorized supervisors every six months.	On Track-Completion Date 4/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-18	**Recertification of Accounts**	**Weakness:** Not recertifying accounts can lead to accounts of terminated employee and contractors remaining active on the system. This can lead to unauthorized access to programs using accounts that should no longer have access to the system. Also, without reviewing access to the shared data and drives, the risk exists that accounts can maintain access to shared data to which they no longer require access. **Recommendation:** A. CBP develop formal procedures for recertifying accounts and access to shared data. B. CBP perform regular re-certifications of accounts and access to shared data as required by developed procedures.	CBP is implementing the use of scripts to disable accounts that have not been used in 30 days. CBP is creating a listing of users produced by . This list will be reduced by those users validated as legitimate by the account re-validation effort. It will be assumed that a user with a validated need to access his/her account, has also been validated to utilize the very network needed to obtain connectivity. Each remaining user will have their supervisor identified via a HR application. Individual supervisors will be contacted via e-mail and asked to verify the employees need to retain an active account.	On Track-Completion Date 9/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-21	**Review of changes to security profiles in**	**Weakness:** Without independent review of security level changes for users, users may be granted additional access they do not need for their job function. In addition, without independent review of these logs by management, security administrators have the ability to make changes to user's access without proper approvals. **Recommendation:** CBP review of these logs should be implemented on a periodic basis by an independent reviewer and that CBP formalize these procedures in detail for the review of security audit logs.	An Information Systems Security Officer/independent reviewer is reviewing the logs on a periodic basis. The logs and evidence of review are to be documented monthly and maintained for seven years.	On Track-Completion Date 6/15/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-26	**Review of Security Violation Logs**	**Weakness:** Without maintaining documented evidence of review for security violation logs per DHS policy, potential access violations could go undetected and these access violations could continue. During a disaster or interruption of service, the restoration of the financial system without pertinent audit information would be challenging. **Recommendation:** CBP follow DHS policy and maintain documented evidence of review for security violation logs for the duration outlined in DHS policy.	CBP has developed an automated electronic system to facilitate the review of the security violation logs and documentation by the security administrators.	Completed-9/17/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High *however Consolidated statement said Medium*	CBP-IT-08-27	**Administrator Access Authorization Weaknesses**	**Weakness:** Without proper authorization granted, the risk exists that personnel may gain access to administrative capabilities without the need to have that access. This could lead to a compromise of data and system functionality. **Recommendation:** A.CBP develop and implement procedures to restrict access to administrative capabilities B. CBP require documented authorization request and approval for each person requiring access to the administrative capabilities.	a. CBP is establishing a project plan to implement an appropriate solution for proper management of the CBP administrative access. This will include the possibility of purchasing software. The Vendor's recommendation may or may not effect the resources requirement. b. CBP will also develop and implement procedures that appropriately restrict access to the administrative capabilities. As well as update the mandatory recertification process to indicate user is a security administrator.	On Track-Completion Date 2/15/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-28	**Completion of [redacted] Access Authorization Forms**	**Weakness:** Without documented authorization, it is possible that users will obtain access to the [redacted], as well as shared drives and folders, without proper authorization. **Recommendation:** CBP continue efforts to develop a method for tracking and consolidating access request forms for the [redacted] and continue to implement the procedures developed to control [redacted] account creation.	Access authorization policies and procedures were developed during FY 2008 but were not fully implemented. The policies and procedures will be fully implemented on or about 3/30/09 .The procedure requires completion of a [redacted] Form for all [redacted]. The Government Supervisor must complete and sign the form in order to obtain new [redacted] accounts or change an active account. The completed forms will be retained in a database which can be audited.	On Track- Completion Date 3/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-29	**Completion of Government Employee Separation Forms**	**Weakness:** Without following the standard procedures for terminating employees from CBP, it is possible that [redacted] will not receive notification that an employee's system access should be removed, leaving accounts active that once belonged to terminated employees. **Recommendation:** CBP require managers to consistently complete the CBP-241 forms that are required as set forth in the CBP directives and policy.	CBP/OF reviewed and revised the CBP Directive No. 51715-005A, "Separation Clearance procedures and CBP Form 242, and disseminated CBP wide. CBP/OF is conducting semi-annual internal reviews to ensure CBP Form is properly completed for all separated employees. The first review of the procedures was conducted from October 2007 to April 2008. The August 19, 2008 report was provided January 7, 2009 and it was determined that compliance with the separation clearance is not being achieved. CBP/OF has not determined what corrective actions will be taken yet.	**The Responsibility for remediation of this finding is Office of Finance**

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however, Consolidated statement said Low***	CBP-IT-08-34	**Installation of Virus Protection on CBP Workstations**	**Weakness:** Without up-to-date antivirus protection on all CBP workstations, the risk exists that malicious code can be introduced to the network and affect a portion of the CBP-maintained workstations. **Recommendation:** CBP develop procedures to regularly review and monitor the workstations that have antivirus protection installed and perform inquiries to determine why identified workstations do not have the protection installed and updated.	CBP is working to ensure that new and existing workstations are added to the CBP domain which will allow all workstations to be accounted for and updated in the appropriate manner. CBP is implementing a process to ensure that Tivoli Endpoints are on all workstations.	On Track-Completion Date 2/28/09
High	CBP-IT-08-35.1	**Configuration management weaknesses on the and application servers and)**	**Weakness:** Weak passwords may allow a remote user to gain unauthorized access on these databases. **Recommendation:** CBP ensure that all database accounts have strong passwords.	CBP is investigating processes to ensure that all database accounts have strong passwords. One such process is that for the weak local account that used has been changed to a more standardize password that meets security standards.	On Track-Completion Date 4/1/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.2	**Configuration management weaknesses on the and application servers and**	**Weakness:** Weak passwords may allow remote user to gain unauthorized access on these databases. **Recommendation:** CBP ensure that all database accounts have strong passwords.	CBP formed a working group to determine what the process will be to change the current password requirements. CBP submit a that will notify all applications utilizing that passwords will need to be strengthened. System owner will provide written details of appliance and its use for demo purposes. If it is determined that demo equipment follows the DHS , system owner will update to password. – This server has been decommissioned.	On Track-Completion Date 12/20/09
High	CBP-IT-08-35.3	**Configuration management weaknesses on the and application servers and)**	**Weakness:** Compromised local administrator passwords allow remote users to gain unauthorized access on the host. **Recommendation**: CBP ensure that all local administrator account passwords adhere to DHS password policy.	CBP changed the patching for the local administrator account.	Completed-11/18/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.4	**Configuration management weaknesses on the and application servers and**	**Weakness:** is installed with a set of well-known usernames and passwords. If the default username and password has not been changed, an attacker can easily break into a database. **Recommendation:** CBP change any default usernames and passwords.	CBP has changed the passwords as follow: For the passwords was changed on and for	Completed 1/22/09
High	CBP-IT-08-35.5	**Configuration management weaknesses on the and application servers and**	**Weakness:** provides a method of calling function outside the database by creating external procedure servers This feature is very useful and extends s functionality greatly, but if access to send commands to these external procedure servers is not properly restricted, anonymous users can gain control of the operating system. **Recommendations:** CBP configure the listener used by the to only accept connections from the database by setting the parameter in the file to restrict access to an Oracle database based on network address.	CBP non-concurred with the finding. Item#5 which deals with , CBP is now using , and is requesting a waiver..	Completed-12/23/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.6	**Configuration management weaknesses on the and application servers and**	**Weakness:** provides a facility to record the actions taken in the database. Recording these actions is necessary in order to detect when an attack occurs and to be able to analyze the attack after the fact. To enable this feature you must set the parameter in the . **Recommendation:** CBP enable auditing.	CBP have researched this discrepancy with the vendor does not agree with the recommendation. The cost, storage and performance issues would be greater risks to the users than acceptance of this risk. CBP will submit a Risk Acceptance Form and waiver for approval. CBP has decided to accept the risk because the risk identified is already being addressed in an alternative manner by the system.	On Track-Completion Date 2/28/09
High	CBP-IT-08-35.7	**Configuration management weaknesses on the and application servers and**	**Weakness:** The parameter allows the database to trust that the client has properly authenticated the user and is who he/she claims to be. If an attacker can identify a user that is configured to use operating system authentication, the attacker will be able to connect to the account without using providing authentication credentials. **Recommendation:** CBP disable client-side authentication.	CBP implemented SAP recommendation into	Completed 1/22/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.8	**Configuration management weaknesses on the and application servers and)**	**Weakness:** provides a facility to record the actions taken in the database. Recording these actions is necessary in order to detect when an attack occurs and to be able to analyze the attack after the fact. Recording when and from where users are connecting or attempting to connect is on the most important features in auditing. **Recommendation:** CBP configure the database to audit both successful and failed connections for all database users.	Upon further research with the vendor does not concur with the recommendation. recommends that this resolution not be implemented as cost, storage, and performance issues would be higher risks to the users than the acceptance of this risk. CBP has decided to accept the risk because the risk identified by the auditor is already being addressed in an alternative manner by the system. Connection is controlled by the application and has extensive functions for logging user activities and changes to the system, and users must connect through the system to access any data in its database. CBP will submit a Risk Acceptance Form and waiver for approval.	On Track-Completion Date 2/28/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.9	**Configuration management weaknesses on the and application servers and**	**Weakness:** The parameter defines the maximum lifetime for passwords. Changing passwords on a regular basis alleviates the threat that passwords have been compromised. If this parameter is set too high or not set at all, old passwords may be compromised and remain in use for an extended period of time. **Recommendation:** CBP set password life time parameter.	CBP initially concurred with the recommendation, however after further researching the issue with the vendor, CBP discovered that the proposed recommendation does not follow the vendor standards. CBP has decided to accept the risked identified by the Auditor, and will submit a Risk Acceptance Form and waiver for approval.	On Track-Completion Date 2/28/09
High	CBP-IT-08-35.10	**Configuration management weaknesses on the and application servers and**	**Weakness:** Passwords need to be changed frequently, as there are many ways to have a password stolen, sniffed and viewed. **Recommendation:** CBP ensure that passwords are reset as mandated by DHS policy.	For the the recommended account changes will be implemented into production by March 31st, 2009.	On Track-Completion Date 3/31/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.11	**Configuration management weaknesses on the and application servers and**	**Weakness:** Obsolete virus definition files may allow an infection of the remote host by a virus or a worm. **Recommendation:** CBP ensure that all virus definition files are up-to-date.	CBP implemented Change Request on 10/14/2008 to enable automated Signature updates. automatically connects to a CBP server hosting the latest signatures and applies them to the appropriate systems.	Completed-11/17/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.12	**Configuration management weaknesses on the and application servers and General Support Systems (GSS)**	**Weakness:** is no longer supported by therefore is vulnerable to multiple remotely exploitable vulnerabilities which may allow an attacker or a worm to take the complete control of the remote system (**Recommendation**: CBP upgrade operating system.	Neither system addressed in this finding is running Systems are running an embedded operating system distributed by on their storage appliance. As such these systems are not susceptible to Windows vulnerabilities Two were reported for the in Aug 2005 (data encompasses 2003 to 2008). The reportedly affect versions prior to versions , and . CBP's devices are thus not susceptible.	Completed-12/18/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-35.13	**Configuration management weaknesses on the and application servers and**	**Weakness:** Obsolete passwords increase the potential for unauthorized access on the host. **Recommendation:** CBP ensure all password parameters meet DHS requirements.	The account is required for mainframe access to to Treasury Files for processing. This process will be changing to use in early 2009 and the account will be eliminated. In the interim CBP is testing a method for locking down the account so that only the can log in with this account and only perform the process. CBP is developing and implementing a policy for changing root and accounts password. Request waiver for user " " from DHS. Implement script developed to change passwords for account on all servers.	On Track-Completion Date 5/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-36.1	**Patch management weaknesses on the and application servers and**	**Weakness:** Multiple high risk vulnerabilities have been addressed in the released . Exploitation of these vulnerabilities will allow an attacker to completely compromise the database. **Recommendation:** CBP apply current	CBP upgrade to version and apply Patch in on 1/18/09. For , no action required as is phasing out the application and no longer support upgrades, including Upgrades and Patches. CBP is retiring this application by 12/31/2009.	On Track- Completion Date 12/31/09
High	CBP-IT-08-36.2	**Patch management weaknesses on the and application servers and**	**Weakness:** An attacker may use these vulnerabilities to execute arbitrary commands on the remote host. **Recommendation:** CBP apply vendor supplied patches.	now has an automated process for patch updates based on Update Services Updates are automatically pulled from a CBP server as they become available and applied to all systems.	Completed- 11/21/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-36.3	**Patch management weaknesses on the and application servers and**	**Weakness:** Allowing database users to access operating system files may result in security being breached. By default, permissions to execute this function are granted to the public role, allowing all users to execute the functions of in the package. **Recommendations:** CBP revoke the privilege to execute the sys.utl_file package from the public role. Grant privileges to execute the package only to those specific accounts that need to execute the package.	For revoking execute of SYS from the PUBLIC Role is in Production	Completed 1/22/09
High	CBP-IT-08-36.5	**Patch management weaknesses on the and application servers and**	**Weakness:** An attacker may be able to execute arbitrary code using malicious file. **Recommendation:** CBP upgrade to Adobe Reader 6.0.6/ 7.0.9/ 8.0 or later.	Upgrade to the latest version. , Adobe Reader will be upgraded. For and is phasing out the application and no longer support upgrades, including Reader. The application will not operate if Reader is upgraded.	On Track- Completion Date 12/31/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-36.6	**Patch management weaknesses on the and P application servers and**	**Weakness:** An attacker may be able to execute arbitrary code on the host. **Recommendation:** CBP update WinZip software.	Upgrade to the and the will be upgraded by 2/15/09. For wil be upgraded on the Production by 2/15/09.	Completed 2/18/09
High	CBP-IT-08-36.7	**Patch management weaknesses on the and application servers and**	**Weakness:** An attacker may be able to execute arbitrary code on the host. Successful exploitation allows an attacker to execute arbitrary code on the affected host subject to the user's privilege. **Recommendation:** CBP update software.	CBP removed Software from all identified workstations.	Completed-11/17/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-36.8	**Patch management weaknesses on the and application servers and**	**Weakness:** The may allow an untrusted applet to elevate its privileges to, for example, read or write local files or to execute local applications subject to the privileges of the user running the applet. Also, another set of vulnerabilities may allow an untrusted applet to access data in other applets. **Recommendation:** CBP upgrade to and or later and remove if necessary any affected versions.	CBP is planning on upgrading to the latest version.	Completed 2/18/09
High	CBP-IT-08-36.9	**Patch management weaknesses on the and application servers and**	**Weakness:** By convincing a user to visit a site with specially-crafted file, an attacker may be able to execute arbitrary code on the affected host or cause the web browser to crash. **Recommendation:** CBP upgrade to or later.	For has been upgraded on the For the Project Shared Drive Flash Player was upgraded.	Completed 1/22/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High	CBP-IT-08-36.10	**Patch management weaknesses on the and application servers and**	**Weakness:** An attacker may use an untrusted application or applet to elevate its privilege by granting itself permission to read and write local files or execute local applications subject to the privileges of the user running the application or applet. **Recommendation:** CBP upgrade to or later and remove any affected versions.	CBP has upgraded to the latest version.	Completed 1/22/09
High	CBP-IT-08-36.11	**Patch management weaknesses on the and application servers and**	**Weakness:** An attacker may be able to exploit this vulnerability by creating a malicious to compromise the computer. In addition, a denial of service vulnerability is present in the remote version of the . An attacker could exploit it by creating an applet which misuses the serialization. **Recommendation:** CBP upgrade to	CBP is planning on upgrading to the latest version.	Completed 2/15/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-37	**Security Violation Review Process**	**Weakness:** By not having formal procedures that document the current review process for security violations, the network security specialist could leave their position and their replacement would not be able to perform the tasks without formal procedures, thereby increasing the risk of undetected security violations. **Recommendation:** CBP create formal procedures to document the mainframe security violation review process.	The procedures for reviewing of the mainframe security logs existed and have been formalized approved, published. And implemented	Completed-11/21/08
Medium ***however Consolidated statement said Low***	CBP-IT-08-38	**Process for reviewing Audit and**	**Weakness:** Without formal procedures in place, the review of audit and may not be performed in a consistent, uniform manner, which may ultimately lead to potential security violations going undetected. **Recommendation:** CBP create formal procedures to document the review process for audit and .	The Information Systems Security Officer(s) have established a folder to act as the central repository for housing these procedures. The access to this repository is limited strictly to those who need to know.	Completed-8/17/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-39	**Password configuration weakness for**	**Weakness:** Without password parameters that are compliant with the organizations policies, there is an increased risk that unauthorized users may be able to guess passwords and gain unauthorized access. **Recommendation:** CBP follow DHS policy and improve password complexity by including special characters for the application.	CBP has established and implemented a new password rules policy in accordance with DHS Policy.	Completed-9/02/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High *however Consolidated statement said Low*	CBP-IT-08-40	**ISSM Approval of Emergency and Temporary Access Authorizations**	**Weakness:** Not having emergency and temporary access approved by the Information Systems Security Manager (ISSM), CBP is not in compliance with DHS policy and is presented with the risk that excessive emergency access to may be granted. **Recommendation:** A. CBP adjust CBP-level and level policies to require the ISSM to approve the emergency and temporary access authorizations prior to access being granted. B. CBP require documented supervisory approval form the ISSM each time a user requires emergency access abilities.	CBP has notified the programs that the CISO must approve list of supervisors who can approve emergency access as well as approving the current list of people with access and their profiles. For all CFO Designated Financial Systems the CISO was provided lists of all emergency access profiles, all developers who have emergency access, and all supervisors authorized to approve emergency access. CISO sent out delegation letters to the owners of the financial systems delegating authority to specific supervisors so they can approve emergency access requests all CFO Designated Financial Systems for 24 hours at a time, no more than 4 times a month per person, for one year. The CISO will re-certify the list of authorized supervisors every six months.	On Track-Completion Date 4/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-41	**Weaknesses in the Process of Separating CBP Contractors**	**Weakness:** By not documenting up-to-date policies for the separation of CBP contractors, the risk exists that contractors will not be separated according to proper policies as outlines by DHS. Also, inconsistent completion of the CBP-242 forms leads to the increased risk that a separating contractor system access will not be deactivated. **Recommendation:** A. CBP document an up-to-date review of this document and make modifications as needed based on the new operating environment for CBP as apart of DHS. B. CBP require the consistent and accurate completion of CBP-242 forms for all separating contractors.	A. CBP has implemented the approved policy directive requiring use of CTS CBP-wide has been distributed by OF and can be found on the workforce management web page. B CBP has implemented the) to facilitate the timely removal of contractor logical and physical access accounts upon their separation from a CBP contract.	Completed 1/22/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Not Rated	CBP-IT-08-42	**Formal agreement not in place for CBP's use of s as Business Continuity facility**	**Weakness:** By not having a complete, signed and up-to date agreement with the business continuity facility provider, CBP is at risk of not having an adequate facility in place to service as a business continuity facility in the event the is rendered inoperable and operations must be moved to an alternate site. **Recommendation:** CBP communicate with DHS and the US Navy to document and Memorandum of Understanding outlining CBP's specific requirements for their business continuity facility and ensure that the agreement is complete, signed and up-to-date.	Stewardship of the has been transferred from CBP to DHS. CBP has provided its requirements to DHS. DHS is responsible for establishing and managing the agreements with the US Navy.	**This NFR was transferred to DHS**

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
High *however Consolidated statement said Medium*	CBP-IT-08-43	**Inadequate Resources at for Business Continuity Testing**	**Weakness:** Inadequate hardware in place for business continuity testing presents CBP the risk that they are unable to fully test business continuity plan and do not have assurance that the plan is appropriately designed and documented. **Recommendation:** CBP allocate the appropriate hardware to , allowing system availability to fully test the business continuity plan to ensure that has the capability to support CBP in the event that the is rendered unavailable for production.	Through the initiative, the continuity posture of CBP will be greatly enhanced at to include infrastructure upgrades and software licensing. The new enhancements will bring the current environment up to a comparable state to that of the production environment at . The deficiencies identified are expected to be addressed as part of the program and CBP infrastructure initiatives over the next 12 months.	On Track- Completion Date 7/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-44	**Completion of Non-Disclosure Agreements for US CBP Contractors**	**Weakness:** By not having contractors sign non-disclosure agreements, the risk exists that individuals may not be aware of their requirements in protecting sensitive DHS and CBP information. **Recommendation:** CBP enforce DHS requirement that a non-disclosure agreement be signed by all contractors in a moderate and high risk level position to ensure that they are aware of their responsibilities in protecting the confidentiality of DHS and CBP data.	CBP/Procurement made procedural changes to the COTR Appointment Memo outlining the responsibilities of the COTR. The COTR is responsible for ensuring that all the contractor complete the DHS Form 11000-6 Non-Disclosure Agreement pursuant to DHS Management Directive 11042.1	Completed 1/28/09
Medium ***however Consolidated statement said Low***	CBP-IT-08-45	**Log configuration weakness for**	**Weakness:** Without correct configuration of the logs to capture appropriate data, actual violations could occur and go undetected. **Recommendation:** CBP properly configure to capture appropriate data for the system.	Corrective action was taken on August 13 2008 to properly configure audit and to capture appropriate data for the . Evidence was provided on 10/02/08.	Completed-10/02/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-46	**Review of Audit and Logs**	**Weakness:** By not maintaining audit and per DHS policy, potential access violations for those specific dates could go undetected and these access violations could continue. **Recommendation:** CBP maintain audit and per DHS policy.	CBP has developed and implemented formal procedures for the review process of . The Mainframe ISSO(s) established a folder for housing these procedures and access is limited to those with a need to know.	Completed-9/18/08
Medium ***however Consolidated statement said Low***	CBP-IT-08-47	**Rules of behavior are not signed before gaining systems access**	**Weakness:** Without signed rules of behavior, CBP management has no formal recourse for holding individuals accountable for their actions on CBP information systems. **Recommendation:** CBP require all CBP personnel (employees and contractors) to sign rules of behavior prior to being granted any system access. For personnel that already have system access, CBP should prioritize having these individual sign rules of behavior to maintain their system access.	CBP has included the DHS Rules of Behavior in all of its mandatory online security training courses and its annual security awareness refresher courses. However, formal acknowledgement has not been required. The Chief Information Security Officer is working with all CBP offices to implement a formal acknowledgment process nationally.	On Track-Completion Date 5/01/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium ***however Consolidated statement said Low***	CBP-IT-08-48	**Security Audit Logs Procedures Weakness**	**Weakness:** By not having detailed procedures that document the review process, the Information Systems Security Officer could leave their position and replacement would not be able to perform the tasks without detailed procedures. **Recommendation:** CBP create detailed procedures that document the review process for security audit logs which includes the documented evidence of review.	The Audit Logs Procedures will be modified to include the evidence of review, sampling methodology and frequency of the review.	On Track-Completion Date 6/15/09
Medium	CBP-IT-08-49	**Weak Initial Password Granted for New Accounts**	**Weakness:** By establishing a weak initial password, the risk exists that a new account's password will be guessed by someone other than the owner of the account and the account will be used inappropriately. **Recommendation:** CBP update the Security Administrator Handbook to require a strong password that is in compliance with DHS and CBP password policies to be set as the initial password for all new account users.	The handbook as well as the password will be changed to meet DHS guidelines.	On Track-Completion Date 3/15/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Low	CBP-IT-08-50	**Inadequate Tracking of Security Awareness Completion**	**Weakness:** By not consistently monitoring completion of security awareness training completion for CBP personnel, the risk exist that persons who have not completed security awareness training will maintain systems access. **Recommendation:** CBP develop a method for determining individuals who have and have not completed security awareness so that they can actively work towards 100% compliance with the DHS requirement, that all individuals with systems access complete annual security awareness training.	The method of tracking completion of security training was inadequate to assure efficient management and deny access to those who did not complete the training. CBP created a report that reads the CBP and searches for all current, active employees (government and contractor) and runs that list against the . The report lists who has not taken specific classes or tests at the time of report generation. CBP created an on-demand dashboard functionality (screen) that is available to OIT to run these reports. This will enable the user to execute the report as needed.	Completed-09/30/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Low	CBP-IT-08-51	**No Document Hardware Maintenance Procedures**	**Weakness:** Without formally documented maintenance procedures for the environment, the risk exists that hardware will not be maintained in a consistent manner, which would lead to the risk that hardware will fail and cause system availability interruptions. **Recommendation:** CBP document their hardware maintenance procedures to ensure a consistent application of maintenance methodologies for the environment.	Corrective actions have been completed. UNIX hardware Maintenance Procedures have been documented and are being followed.	Completed-11/17/08

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Low	CBP-IT-08-52	**Screensavers are not appropriately configures on the**	**Weakness:** By not configuring screensavers to automatically activate after 5 minutes of inactivity, the risk exists that unattended systems will be used by individuals other than the one who is logged into the unattended system. **Recommendation:** CBP determine a method for appropriately applying CBP and DHS policy requiring automatically-activated password-protected screensavers after a period of activity.	CBP reviewing current policy on screensavers and vet through all CBP ACs to determine if an exception is necessary. An exception was determined to be necessary, draft exception request to increase time out for screensaver activation from 5 minutes to 15 minutes. CBP obtained signature on exception. This solution will also disable the function whereby any individual could change the length of activation time on their screensavers. We estimate this process to take around four months.	On Track-Completion Date 4/30/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Low	CBP-IT-08-53	**Out of Date and Inaccurate Security Administrator Handbook**	**Weakness:** By maintaining an out of date Security Administrators Handbook, the risk exists that Security Administrators will improperly perform their duties or tasks that are not in compliance with DHS and CBP policies. **Recommendation:** CBP conduct a full review of the Security Administrators Handbook needs to be performed and updates made to the document that reflects the current operating environment. The review should be documented and the Handbook should include a change log as evidence of the updates that were made.	The handbook is in the process of being updated and approved will be completed by February15, 2009.	On Track-Completion Date 3/15/09
Medium	CBP-IT-08-54	**Access Control Policies and Procedures Weaknesses**	**Weakness:** Without formally documented access control policies and procedures and implementation of these procedures, the risk exists that access to functionality and data will not be consistently controlled at the various ports where it is used. **Recommendation:** CBP document and implement policies and procedures for access control.	CBP is establishing and implementing policies and procedures for access control. will implement a new automated process for recertification every six months for all users, document a formal process for the creation of portal users and configure to lockout user's account after 45 days of inactivity.	On Track-Completion Date 8/31/09

Risk Rating	NFR Number[1]	NFR Title	Detailed Weakness/ Recommendation	Planned Corrective Actions	Status/ Scheduled Completion Date
Medium	CBP-IT-08-55	**Consistency in Creation of Accounts and Administrator Accounts**	**Weakness:** By not controlling the way in which accounts are created, the risk exists that accounts will be created in an inappropriate and unauthorized manner. **Recommendation:** CBP limit the organization that can create accounts, administrator accounts and require any accounts created to be created by a singular organization.	CBP procured and installing third party software tool (e.g. or equivalent) to support access control. Contact entities other than ENTS Field Support who granted and remind them of existing procedures that requires coordination with Field Support and completion of the standard access request forms for any individuals with access that has not been documented with ENTS Field Support. Using the software tool procured, produce periodic reports to determine if accesses are being granted in compliance with the requirement for centralized documentation.	On Track- Completion Date 5/30/09

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
Under Secretary, Management
Commissioner, CBP
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, CBP
Chief Information Officer, CBP
DHS Chief Information Security Officer
Assistant Secretary, Policy
Assistant Secretary for Public Affair
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, please 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.