Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2009 U.S. Customs and Border Protection (CBP) Financial Statement Audit (Redacted)

OIG-10-109

August 2010

Office of Inspector General

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

Homeland Security

AUG 11 2010

Preface

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

This report presents the information technology (IT) management letter for the U.S. Customs and Border Protection component of the FY 2009 DHS financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report, November 13, 2009 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 2009 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated January 22, 2010, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036

January 6, 2010

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
Customs and Border Protection

Ladies and Gentlemen:

We have audited the consolidated balance sheets of the Customs and Border Protection (CBP), a component of the U.S. Department of Homeland Security (DHS), as of September 30, 2009 and 2008, and the related consolidated statements of net cost, changes in net position, custodial activity, and the combined statement of budgetary resources (referred to herein as "consolidated financial statements") for the years then ended. In planning and performing our audit of the consolidated financial statements of CBP, in accordance with auditing standards generally accepted in the United States of America, we considered CBP's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements but not for the purpose of expressing an opinion on the effectiveness of CBP's internal control. Accordingly, we do not express an opinion on the effectiveness of CBP's internal control. In planning and performing our fiscal year 2009 audit, we considered CBP's internal control over financial reporting by obtaining an understanding of the design effectiveness of CBP's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements. To achieve this purpose, we did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*. The objective of our audit was not to express 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 deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our audit of CBP as of, and for the year ended, September 30, 2009 disclosed a material weakness in the areas of Information Technology (IT) access controls, security management, and segregation of duties. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated January 6, 2010. This letter represents the separate restricted distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management and communicated through a Notice of Finding and Recommendation (NFR), and are intended **For Official Use Only**. Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim to use our knowledge of related to CBP gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key CBP financial systems and IT infrastructure within the scope of the FY 2009 CBP consolidated financial statement audit in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to certain additional matters have been presented in a separate letter to the Office of Inspector General and the CBP Chief Financial Officer dated January 6, 2010.

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

KPMG LLP

Very truly yours,

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

We have audited the consolidated balance sheets of the United States (U.S.) Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP) as of September 30, 2009, and related consolidated statements of net cost, changes in net position, custodial activity, and the combined statements 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 Information Technology (IT) general controls of CBP's financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit as it relates to the IT general control assessment at CBP. The scope of the IT general controls assessment is described in Appendix A.

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.

- *Security management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit, we also performed technical security testing for key network and system devices. The technical security testing was performed 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. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

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

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2009, CBP took corrective action to address many prior-year IT control deficiencies. For example, CBP made improvements in the tracking of security awareness completion, the controlling of emergency and temporary access to Automated Commercial System (ACS), and the recertification of National Data Center (NDC) Local Area Network (LAN) accounts. However, during FY 2009, we continued to identify IT general control deficiencies at CBP. The most significant deficiencies from a financial statement audit perspective related to controls over access to programs and data. Collectively, the IT control deficiencies 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 deficiencies 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 IT findings were combined into one significant deficiency regarding IT for the FY 2009 audit of the CBP consolidated financial statements.

Although we noted improvement, the conditions identified at CBP in FY 2008 have not been completely addressed because CBP still faces challenges related to the merging of numerous IT functions, controls, processes, and organizational resource shortages. During FY 2009, CBP took steps to address these conditions. Despite these improvements, CBP needs further emphasis on the monitoring and enforcement of access controls as well as implementing and enforcing the CBP-wide security certification and accreditation (C&A) program. Many of the issues identified during our review, which were also identified during FY 2008 and prior can be addressed through a more consistent and effective security C&A program and security training program.

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

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

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

Conditions: In FY 2009, the following IT and financial system control deficiencies were identified at CBP. Several of the issues identified during our FY 2009 engagement were also identified during FY 2008. The following IT and financial system control deficiencies contribute to a significant deficiency for financial system security.

Access Controls – we noted:

1. The log of ACS access profile changes is not regularly reviewed by personnel independent from those individuals that have made the changes.

2. CBP does not maintain authorizations for personnel that have administrator access to .

3. Parameters for all mainframe audit and system utility logs are not configured to collect appropriate data.

4. The following issues in regard to ACS Security Profile Change Log Procedures:

    a. Procedures do not define how often the ACS security profile change audit logs are reviewed;
    b. Procedures do not describe how evidence of the review process is created by the ACS Information System Security Officer (ISSO)/Independent Reviewer; and
    c. Procedures do not define the sampling methodology that is used to select ACS profile change security logs for review.

5. Automated Commercial Environment (ACE) audit logs are not being reviewed on a regular basis.

6. A total of 5 out of the 25 sampled NDC LAN audit logs were either blank or did not contain pertinent audit log information.

7. passwords were not required to be case sensitive for approximately half the fiscal year and therefore did not meet CBP and DHS requirements.

8. Procedures on how to generate the system utility log reports for the Mainframe ISSO's review do not exist.

9. The control option to limit the number of failed logon attempts to the was not configured properly.

10. was not configured to disable accounts after 45 days of inactivity for the full fiscal year, as required by CBP and DHS policy.

11. ACS Information Security Agreements (ISAs) for all identified participating government agencies have not been documented as required by CBP and DHS policies.

12. Initial access requests and approvals for 30 out of 45 individuals granted access to ACE during FY 2009 could not be provided.

13. portal accounts for separated employees are not timely removed as required by CBP and DHS policy.

14. Access request documentation for individuals who had their ACS access profiles modified during FY 2009 was not consistently maintained.

15. The review of SAP profile changes consisted of only a review of access deletes and did not include a review of additions of new users and modification to user ID's (change/addition of profiles).

16. Certain individuals were not appropriately limited to temporary/emergency access as required by the Chief Information Security Officer (CISO).

17. Certain individuals did not have CISO approval for their emergency access to . Additionally, it was noted that there was one instance in which the emergency access was granted in error without authorization and three instances where the improper form was used to request emergency/temporary access; and,

18. Formal access documentation for 3 ACE National Security Control Officers (SCOs) created in FY 2009 and 37 ACE Field SCOs created in FY 2009 were reviewed. The following exceptions were noted:

    a. Two of the three National SCOs were not authorized and their roles were added in error.
    b. One National SCO was approved through a manual recertification and initial authorization request and/or approval could not be provided.
    c. Thirty-six of the thirty-seven field SCO's initial authorization and approvals could not be provided. While these accounts were approved through the account recertification process, it could not be determined who performed the recertification and what their authorization level was.

Security Management – we noted:

1. A complete and accurate listing . It was noted that the list did not contain accurate .

2. There are a significant number of non- workstations that do not appear on the listing of workstations, as maintained by the administrators, and therefore do not have installed.

3. A complete, up-to-date listing of all CBP workstations is not maintained.

4. Of forty-five selected individuals that had separated in FY 2009, 19 of these individuals did not have a completed CBP-241 form on file.

5. Twenty-four out of 60,750 AD workstations did not have virus protection installed. Additionally, it could not be determined what percentage of non-AD workstations have virus protection installed.

6. A new directive was issued requiring the use of the Contractor Tracking System (CTS). However, this directive refers to Department of Treasury policies, and therefore is outdated as CBP is no longer a part of Treasury. Additionally, CBP-242 contractor separation forms were not appropriately completed for 3 out of 45 selected CBP contractors.

7. Non-Disclosure Agreements (NDAs) for 8 out of 45 selected contractors were signed several months after their hire date. Additionally, one NDA did not have a witness signature, indicating that the NDA was not appropriately completed.

8. There are six individuals within the Office of Information Technology (OIT) that are in critical sensitive positions and have not had their periodic reinvestigations completed within the five year time frame.

9. The requirement to sign a Rules of Behavior (ROB) form is not implemented consistently. Specifically, 10 out of 40 selected individuals with systems access do not have a signed ROB form on record. Additionally, 11 individuals signed the ROB form months after the requirement was implemented.

10. During our technical testing, configuration and patch management exceptions were identified on AD Domain Controllers and hosts supporting the SAP and ACE applications.

Segregation of Duties – we noted:

1. is not currently configured to restrict access to least privilege for performing job functionality as required by CBP policy.

Other Findings in IT General Controls

After-Hours Physical Security Testing

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a CBP employee's/contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various CBP locations that process and /or maintain financial data as shown in the following table.

Security Weaknesses Observed During After Hours Physical Security Testing					
	CBP Locations				
Exceptions Noted	**Building**	**Building**	**Building**	**Building**	**Total Exceptions by Type**
Passwords	0	7	2	1	**10**
For Official Use Only (FOUO) Documents	1	4	8	13	**26**
Keys/Badges	3	2	1	1	**7**
Personally Identifiable Information (PII)	7	7	5	3	**22**
Server Names/IP Addresses	0	2	0	0	**2**
Unsecured Laptops	0	1	1	1	**3**
Unsecured External Drives	0	0	0	4	**4**
Credit Cards	0	0	0	2	**2**
Classified Documents	0	0	0	0	**0**
Other –U.S. Government official passport	0	0	0	1	**1**
Total Exceptions by Location	**11**	**23**	**17**	**26**	**77**
Source: CBP management and KPMG direct observation and inspection of work areas.					

Note that approximately 15 desks / offices were examined for each one of the columns in the above table.

Social Engineering Testing

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to deception for the purpose of information gathering, or gaining computer system access.

Locations	Total Called	Total Answered	Number of people who provided a password
CBP Sites	30	10	2

Recommendations: We recommend that the CBP OIT, in coordination with the Office of Finance (OF), make the following improvements to the CBP financial management systems and processes.

For access controls, we recommend that CBP:

1. Implement the review of ACS profile change logs on a periodic basis by an independent reviewer and that CBP formalize the procedures in detail for the review of ACS security profile change logs.

2. Implement procedures that have been developed to restrict access to mainframe administrative capabilities and require documented authorization requests and approval for each person requiring access to the mainframe administrative capabilities.

3. Properly configure mainframe audit and system utility logs to capture appropriate data for the NDC Mainframe system.

4. Create detailed procedures that document the review process for ACS profile change logs that includes the documented evidence of review.

5. Implement the procedures that have been established for reviewing ACE audit logs on a weekly basis to be in compliance with DHS guidelines.

6. Conduct a more thorough review of NDC LAN audit logs to ensure that logs are capturing all necessary information and that no blank logs exist. Further, CBP must ensure that audit logs are configured properly to capture all information and activity on the system.

7. Create and implement formal procedures to document the generation of mainframe audit and system utility logs.

8. Adjust the control option in the to result in the immediate suspension of any user who exceeds the specified number of violations, which should be set a reasonably low number.

9. Modify appropriately to ensure that accounts are disabled after 45 days of inactivity.

10. Develop a consistent and uniform naming scheme for all current and future ACS connections to facilitate the identification of all existing ACS connections as well as to facilitate in the reconciliation of existing ISAs. Once all ACS mission connections have been identified, that the appropriate ISAs are produced.

11. Implement procedures to consistently document the access requests and approvals for any and all access creations and changes to ACE users.

12. Investigate and implement a method to disable CBP accounts for separated employees and contractors upon their separation or before, as determined appropriate by security management and Human Resources.

13. Implement procedures to consistently document the access requests and approvals for any and all access creations and changes to ACS user profiles.

14. Implement review of access change logs on a periodic basis by an independent reviewer and that CBP modify their procedures to ensure that all types of access changes (adds, deletes and modifications) are reviewed to ensure that appropriate requests and approvals were documented.

15. Formalize procedures around the process for granting temporary and emergency access to developers to ensure that access to these sensitive roles is restricted appropriately. Specifically, CBP should ensure controls are in place to confirm a user is authorized to be granted the role and that the individual had not been granted that role more than authorized by the Component CISO over a certain period of time.

16. Continue to implement processes to appropriately restrict and authorize access to temporary and emergency roles within and,

17. Develop and implement procedures to restrict access to the Field and National SCO roles and require documented authorization requests and approval for each person requiring access to the

For security management, we recommend that CBP:

1. Implement procedures to have regularly reviewed and updated by to ensure the most accurate data is in the for use by all of CBP.

2. Research, identify, and implement a method to consistently account for all CBP workstations and perform regular reviews to ensure that all CBP workstations have Tivoli or some future solution, appropriately applied.

3. Work with administrators across the country to ensure that new and existing workstations are added to a centralized accounting structure such as AD or some other more appropriate solution, if identified, to allow for all workstations to be accounted for in an appropriate fashion.

4. Develop a standardized method of maintaining the CBP-241 forms to ensure that all forms for all separating employees are completed in a timely manner and are easily accessible.

5. Research, identify, and implement a method to consistently account for all CBP workstations and perform regular reviews to ensure that all CBP workstations have virus protection installed and that it is regularly updated.

6. Review the current Customs Directive regarding separation procedures for CBP contractors and update it to reflect the current operating environment. Additionally, CBP should require the consistent and accurate completion of the CBP-242 forms for all separating contractors.

7. Implement a more consistent method of ensuring that contractors sign an NDA. Furthermore, ensure that COTRs regularly review their contractor information and that there is an NDA for each contract under their supervision.

8. Devote adequate resources to the completion of periodic background reinvestigations that are due for all CBP personnel. Additionally, CBP should devote special attention to those individuals in critical sensitive positions requiring initial or periodic reinvestigations.

9. Implement a more consistent method of ensuring that all individuals with CBP systems access sign a ROB form. Also, methods should be developed to ensure that individuals with access to any and all CBP systems have a rules of behavior signed.

10. Review their information system security awareness programs to ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical CBP data and hardware. Additionally, CBP employees and contractors should be made especially aware of the need to protect personally identifiable information as well as information marked "For Official Use Only," and,

11. Address the specific conditions identified in the finding related to configuration and patch management deficiencies.

For segregation of duties, we recommend that:

1. The ACE Security Team continue to work with the Office of Finance to identify incompatible roles and that procedures are developed as part of the access control process to ensure that these role combinations are not granted to ACE users.

Cause/Effect: Several of these deficiencies were a result of either an inadequate allocation of resources to address prior year findings or only partial implementation of recommendations to prior year findings. By not addressing the conditions noted above, the risk exists that deficiencies may be exploited, in either a singular fashion or in combination which might affect the availability, confidentiality or integrity of CBP's financial systems and 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 Office of Management and Budget (OMB) and the National Institute of Standards and Technology (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. 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 2009, we noted that CBP is unable to prevent, or detect and correct excessive drawback claims due to the inherent limitations and the lack of controls therein. Additionally These control deficiencies were presented to CBP management as a material weakness.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from Customs and Border Protection management. Generally, CBP management agreed with our findings and recommendations. CBP management has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments in Appendix D.

OIG Response

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

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2009 CBP Financial Statement Audit

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE

Below is a description of significant United States (U.S.) Customs and Border Protection (CBP) financial management systems and supporting information technology (IT) infrastructure included in the scope of CBP's fiscal year (FY) 2009 Financial Statement Audit.

Locations of Review: The CBP National Data Center (NDC) in

Key Systems Subject to Audit:

- *Systems, Applications, and Products Release 3 (SAP R/3)* - SAP 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. SAP is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the AIMS mainframe-based financial system using a phased approach.

- *Automated Commercial System (ACS)* – ACS 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 ACS includes systems for data input/output, entry and entry summary, and collection of revenue.

- *Automated Commercial Environment (ACE)* – ACE is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. ACE is being deployed in phases, with a final full deployment scheduled for FY 2010. As ACE is partially implemented now and processes a significant amount of revenue for CBP, ACE was included in full scope in the FY 2009 financial statement audit.

- *Seized Assets and Cases Tracking System (SEACATS)* – Used for tracking seized assets, Customs Forfeiture Fund, and fines and penalties.

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

Appendix B

FY 2009 Notices of Information Technology Findings and Recommendations

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

Notices of Findings and Recommendations (NFR) – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the Department of Homeland Security (DHS) *Independent Auditors' Report.*

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist CBP in the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-03	During testing, KPMG was informed that all data had not been completely captured from all organizations within CBP to ensure a complete and accurate listing [redacted] Additionally, through inspection of data on current contractors, KPMG noted that there were data validity issues in the system, [redacted]	KPMG recommends that CBP implement procedures to have [redacted] data regularly reviewed and updated by [redacted] to ensure the most accurate data is in the [redacted] for use by all of CBP.		**X**	**2**
CBP-IT-09-12	KPMG noted that [redacted] is installed on a significant majority of workstations at CBP. These workstations are on the [redacted] system. However, KPMG noted that there are a significant number of non-AD workstations that do not appear on the [redacted] listing of workstations, as maintained by the [redacted] We noted that these workstations do not have [redacted] installed as required.	KPMG recommends that CBP research, identify and implement a method to consistently account for all CBP workstations and perform regular reviews to ensure that all CBP workstations have [redacted] or some future solution, appropriately applied.		**X**	**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-13	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. Specifically, KPMG noted that workstations maintained within AD can be accounted for in a reasonable manner. However, workstations that are not in AD are difficult to account for, as they are not part of the Active Directory structure and can only be identified when connecting to the network, which may not occur regularly (i.e., laptops, unused equipment, etc).	KPMG recommends that CBP work with administrators across the country to ensure that new and existing workstations are added to a centralized accounting structure such as AD or some other more appropriate solution, if identified, to allow for all workstations to be accounted for in an appropriate fashion.		**X**	**2**
CBP-IT-09-21	KPMG noted that when changes to a user's Automated Commercial System (ACS) access profile are performed, the log of these events is not regularly reviewed by personnel independent from those individuals that made the changes.	KPMG recommends that the review of these logs be implemented on a periodic basis by an independent reviewer and that CBP formalize these procedures in detail for the review of ACS security profile change logs.		**X**	**2**
CBP-IT-09-27	KPMG noted that authorizations are still not being maintained for personnel that have administrator access to [redacted] Procedures have been implemented to require documented authorization however evidence could not be provided that these procedures are being implemented appropriately.	KPMG recommends that CBP implement procedures that have been developed to restrict access to mainframe administrative capabilities and require documented authorization requests and approval for each person requiring access to the mainframe administrative capabilities.		**X**	**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-29	KPMG selected 45 individuals that had separated in fiscal year (FY) 2009 and noted that 19 of these individuals did not have a completed CBP-241 form on file. Additionally, KPMG noted that two forms provided for two different individuals were incomplete and lacked a supervisor's signature.	KPMG recommends that CBP develop a standardized method of maintaining the CBP-241 forms to ensure that all forms for all separating employees are completed in a timely manner and are easily accessible.		**X**	**2**
CBP-IT-09-34	KPMG noted that 24 out of 60,750 AD workstations, or 0.04 percent, did not have antivirus installed, which is a negligible amount. However, KPMG could not determine what percentage of non-AD workstations have virus protection installed, as non-AD workstations do not communicate with the ePolicy Orchestrator system that is used to maintain and update virus protection across CBP workstations and networks.	KPMG recommends that CBP research, identify and implement a method to consistently account for all CBP workstations and perform regular reviews to ensure that all CBP workstations have virus protection installed and that it is regularly updated.		**X**	**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-41	KPMG noted that a Customs Directive was provided as separation procedures for contractors and that 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. A new directive was issued requiring the use of the Contractor Tracking System; however, the new directive still refers to the old directive, which has not been updated. Additionally, KPMG noted that CBP-242 contractor separation forms are not completed consistently for separating CBP contractors. Specifically, KPMG noted that 3 separated contractors out of 45 selected had their forms completed over one month after they separated from CBP.	KPMG recommends that CBP review the current Customs Directive and update it to reflect the current operating environment. Additionally, KPMG recommends that CBP require the consistent and accurate completion of the CBP-242 forms for all separating contractors.		**X**	**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-44	While KPMG notes that progress has been made in implementing procedures requiring the signing of non-disclosure agreements, KPMG noted that non-disclosure agreements are still not consistently being signed by contractors at CBP. Specifically, KPMG noted that non-disclosure agreements (NDAs) for 8 out of 45 selected contractors were signed many months after their hire date. Additionally, KPMG noted that one NDA did not have a witness signature, indicating the NDA was not appropriately completed.	KPMG recommends that CBP implement a more consistent method of ensuring that contractors sign an NDA. KPMG also recommends that COTRs regularly review their contractors and ensure that there is an NDA for each contractor under their supervision.		**X**	**2**
CBP-IT-09-45	Parameters for all mainframe audit and system utility logs are not configured to collect appropriate data. Specifically, KPMG noted that one out of the six mainframe audit and system utility logs, , did not produce any data during the time of testing due to an inaccurate filtering configuration.	KPMG recommends that CBP properly configure mainframe audit and system utility logs to capture appropriate data for the National Data Center (NDC) mainframe system.		**X**	**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-48	KPMG noted the following deficiencies related to the ACS Security Audit Logs procedures: • Procedures do not define how often the ACS security profile change audit logs are reviewed. • Procedures do not describe the documented how evidence of the review process is created by the ACS Information System Security Officer (ISSO)/Independent Reviewer. • Procedures do not define the sampling methodology that is used to select ACS profile change security logs for review.	KPMG recommends that CBP create detailed procedures that document the review process for ACS profile change logs that include documented evidence of review.		**X**	**2**
CBP-IT-09-56	KPMG noted that Automated Commercial Environment (ACE) audit logs are not being reviewed on a regular basis. KPMG noted that procedures have been established, which require that audit logs and events be reviewed on a weekly basis. However, at this time, procedures have not been implemented effectively.	KPMG recommends that CBP implement the procedures that have been established for reviewing ACE audit logs on a weekly basis to be in compliance with DHS guidelines.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-57	KPMG noted that 5 out of the 25 sampled audit logs did not contain any audit log information, such as login attempts, intruder detected, login failed, Access Control List (ACL) changed, object activity, etc. KPMG did not receive audit log information for the following five selected dates: • February 16, 2009 • April 1, 2009 • April 7, 2009 • April 19, 2009 • May 4, 2009	KPMG recommends that CBP conduct a more thorough review of audit logs to ensure that logs are capturing all necessary information and that no blank logs exist. Further, CBP must ensure that audit logs are configured properly to capture all information and activity on the system.	**X**		**2**
CBP-IT-09-58	KPMG noted that passwords were not required to be case sensitive for a period of time during our testing and therefore did not meet CBP and DHS requirements. Further testing has shown that passwords currently are required to be case sensitive and that issue has now been resolved.	As this condition was addressed during the course of the audit fieldwork, KPMG has no further recommendation to CBP.	**X**		**2**
CBP-IT-09-59	KPMG noted that formal procedures do not exist that describe the mainframe audit process and how to generate the system utility log reports for the mainframe ISSO's review.	KPMG recommends that CBP create and implement formal procedures to document the generation of mainframe audit and system utility logs.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-60	KPMG noted that one user was allowed 1,476 failed attempts to access a dataset to which they were not authorized before their access was suspended in the . KPMG determined that the control option in the security software, which results in immediate suspension of any user who exceeds the specified number of violations, was not configured properly.	KPMG recommends an adjustment to the Access Response control option to result in the immediate suspension of any user who exceeds the specified number of violations, which should be set at a reasonably low number of attempts.	**X**		**2**
CBP-IT-09-61	KPMG noted that there are six individuals within Office of Information Technology (OIT) that are in critical sensitive positions and have not had their periodic reinvestigations completed within the five year time frame. Specifically, of these six individuals, KPMG noted the following: • Two individuals in critical positions had their reinvestigations completed a year or longer later than they should have been. • Four individuals in critical positions should have had their reinvestigations completed and are several months late. Of these four individuals, one has not had his/her investigation status updated since August 2002.	KPMG recommends that CBP devote adequate resources to the completion of periodic reinvestigations and initial investigations that are due for all CBP personnel. Additionally, KPMG recommends that CBP devote special attention to those individuals in critical sensitive positions requiring initial or periodic reinvestigations.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-62	Significant progress has been made in requiring individuals with systems access to sign a rules of behavior before systems use. KPMG noted however that the requirement to sign a rules of behavior (ROB) form is not implemented consistently. Out of 40 individuals with systems access across the country, 10 individuals did not have a signed ROB form on record. Additionally, 11 individuals signed the ROB form months after the CBP Chief Information Officer (CIO's) requirement to sign the ROB form. These individuals have had access during fiscal year 2009.	KPMG recommends that CBP implement a more consistent method of ensuring that all individuals with CBP systems access sign a ROB form. KPMG also recommends that methods be developed to ensure that individuals with access to any and all CBP systems have a ROB form signed.	**X**		**2**
CBP-IT-09-63	KPMG noted that is not configured to disable accounts after 45 days of inactivity for the full fiscal year, as required by CBP and DHS policy.	KPMG recommends that CBP ensure that the Change Request to implement this control is completed, appropriately approved and implemented to disable accounts after 45 days of inactive as required by CBP and DHS policy.	**X**		**2**
CBP-IT-09-64	KPMG determined that Information Security Agreements (ISAs) for all identified participating government agencies have not been documented as required by CBP and DHS policies.	KPMG recommends that CBP develop a consistent and uniform naming scheme for all current and future ACS connections to facilitate the identification of all existing ACS connections as well as to facilitate in the reconciliation of existing ISAs. Finally, KPMG recommends that once all ACS mission connections have been identified, that the appropriate ISAs be produced.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-65	KPMG inspected access request documentation for 45 individuals who were granted ACE access during FY 2009. Initial access requests and approvals for 30 of these individuals could not be provided. Although confirmation that access is appropriate was provided for these 30 individuals, access approvals prior to the creation of their accounts was not maintained.	KPMG recommends that CBP implement procedures to consistently document the access requests and approvals for any and all access creations and changes to ACE users.	**X**		**2**
CBP-IT-09-66	KPMG noted that CBP portal accounts for separated employees are removed on a bi-weekly basis and are not removed on the day of the individual's separation as required by CBP and DHS policy. Additionally, KPMG noted that one contractor who had access had separated from CBP but the account was not disabled until some time after he/she had separated.	KPMG recommends that CBP investigate and implement a method to disable CBP accounts for separated employees and contractors upon their separation or before, as determined appropriate by security management and Human Resources.	**X**		**2**
CBP-IT-09-67	KPMG inspected access request documentation for 45 individuals who had their access profiles modified during FY 2009. Access change requests and approvals for 14 of these individuals could not be provided. Although confirmation that the access is appropriate was provided for these 14 individuals, access approvals prior to the modification of the account were not maintained.	KPMG recommends that CBP implement procedures to consistently document the access requests and approvals for any and all access creations and changes to user profiles.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-68	During our technical testing, patch and configuration management exceptions were identified on the environment. These conditions can be found in the table within the actual NFR.	During our technical testing, patch and configuration management exceptions were identified in the environment. The recommendations to address these conditions can be found in the table within the actual NFR.	**X**		**2**
CBP-IT-09-69	KPMG inspected profile change reviews performed by CBP management for changes to SAP access profiles and noted that the profile reviews were ineffective. Specifically, KPMG noted that only access deletes were tested in the review. These deletes remove an individual's access and do not increase an individual's access. Additions of new users and modification to user ID's (change/addition of profiles) were not part of the selected access changes that were reviewed. The reviews only consisted of deleted accounts and did not review any new accounts that had been added during the review period.	KPMG recommends that the review of these access change logs is implemented on a periodic basis by an independent reviewer and that CBP modify their procedures to ensure that all types of access changes (adds, deletes and modifications) are reviewed to ensure that appropriate requests and approvals were documented.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-70	KPMG noted that a memo was issued by the Component Chief Information Security Officer (CISO) to limit temporary/emergency access to no more than four times per month. KPMG noted that the policy was adjusted to restrict access to 25 times per user, per role, over a six month period. Taking into account this new control, KPMG noted that during FY 2009, there was one individual who was granted access to a temporary/emergency role 43 times over a six month period.	KPMG recommends that procedures be formalized concerning the process for granting temporary and emergency access to developers to ensure that access to these sensitive roles is restricted appropriately. Specifically, KPMG recommends that CBP ensure controls are in place to confirm a user is authorized to be granted the role and that the individual had not been granted that role more than authorized by the Component CISO over a certain period of time.	**X**		**2**
CBP-IT-09-71	KPMG noted that out of a selected 25 instances in which emergency access was granted to users, 4 individuals did not have CISO approval for their emergency access. Additionally, KPMG noted that there was one instance in which the emergency access was granted in error without authorization and three instances in which an improper form was used to request emergency/temporary access.	KPMG recommends that CBP continue to implement processes to appropriately restrict and authorize access to temporary and emergency roles within .	**X**		**2**
CBP-IT-09-72	KPMG noted that is not currently configured to restrict access to least privilege for performing job functionality as required by CBP policy.	KPMG recommends that the Security Team continue to work with the Office of Finance to identify incompatible roles and that procedures are developed as part of the access control process to ensure that these role combinations are not granted to ACE users.	**X**		**2**

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-73	KPMG inspected access documentation for 3 National Security Control Officers (SCOs) created in FY 2009 and 37 Field SCOs created in FY 2009 and noted the following exceptions: • Two of the three National SCOs were not authorized and their roles were added by mistake. • One National SCO was approved through a manual recertification and initial authorization request and/or approval could not be provided. • Thirty-six of the thirty-seven Field SCO's initial authorization and approval could not be provided. Instead, a recertification was provided, though the recertification did not note who performed the recertification and what authorization they had to perform the recertification.	KPMG recommends that CBP develop and implement procedures to restrict access to the Field and National SCO roles and require documented authorization requests and approval for each person requiring access to ACE administrative capabilities.	**X**		**2**
CBP-IT-09-74	Multiple incidents of unprotected CBP information systems and data were found as a result of physical security walkthroughs. Additionally, passwords were obtained from two CBP employees through social engineering techniques. The details of this testwork can be viewed in the actual NFR.	KPMG recommends that CBP review their information system security awareness programs to ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical CBP data and hardware. Additionally, CBP employees and contractors should be made especially aware of the need to protect personally identifiable information as well as information marked "For Official Use Only."	**X**		**2**

Appendix C

Status of Prior Year Notices of Findings and Recommendations, and, Comparison to Current Year Notices of Findings and Recommendations

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-08-02	Automated Commercial System (ACS) Interconnection Security Agreements (ISAs)	X	
CBP-IT-08-03	Contractor Deficiencies		CBP-IT-09-03
CBP-IT-08-08	National Data Center (NDC) Local Area Network (LAN) Audit Logs	X	
CBP-IT-08-09	Disabling of Inactive Accounts on NDC LAN	X	
CBP-IT-08-12	Installation		CBP-IT-09-12
CBP-IT-08-13	Complete List of Customs and Border Protection (CBP) Workstations		CBP-IT-09-13
CBP-IT-08-16	Excessive ACS Emergency Access	X	
CBP-IT-08-18	Recertification of NDC LAN Accounts	X	
CBP-IT-08-21	Review of Changes to Security Profiles in ACS		CBP-IT-09-21
CBP-IT-08-26	Review of Mainframe Security Violation Logs	X	
CBP-IT-08-27	Administrator Access Authorization Weaknesses		CBP-IT-09-27
CBP-IT-08-28	NDC LAN Access Policies and Procedures	X	
CBP-IT-08-29	Completion of CF-241 Forms for Terminated Employees		CBP-IT-09-29
CBP-IT-08-34	Installation of Virus Protection		CBP-IT-09-34
CBP-IT-08-35	Configuration Management	X	
CBP-IT-08-36	Patch Management	X	
CBP-IT-08-37	Security Violation Review Process	X	
CBP-IT-08-38	Process for Reviewing Mainframe Audit and System Utility Logs	X	
CBP-IT-08-39	Password Configuration Weakness in Automated Commercial Environment (ACE)	X	
CBP-IT-08-40	Information System Security Manager (ISSM) Approval of SAP Emergency	X	

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

NFR No.	Description	Disposition	
		Closed	Repeat
	and Temporary Access Authorizations		
CBP-IT-08-41	Weaknesses in the Process of Separating CBP Contractors		CBP-IT-09-41
CBP-IT-08-43	Inadequate Resources at for Business Continuity Testing	**X**	
CBP-IT-08-44	Completion of Non Disclosure Agreements for CBP Contractors		CBP-IT-09-44
CBP-IT-08-45	Log Configuration Weakness for NDC Mainframe System		CBP-IT-09-45
CBP-IT-08-46	Review of Mainframe Audit and System Utility Logs	**X**	
CBP-IT-08-47	Rules of Behavior Forms are Not Signed Before Gaining Systems Access	**X**	
CBP-IT-08-48	Lack of Effective ACS Access Change Log Review Procedures		CBP-IT-09-48
CBP-IT-08-49	Weak Initial Passwords Granted for New Accounts in ACS	**X**	
CBP-IT-08-50	Inadequate Tracking of Security Awareness Training Completion	**X**	
CBP-IT-08-51	No UNIX Hardware Maintenance Procedures	**X**	
CBP-IT-08-52	Screensavers are Not Appropriately Configured on the NDC LAN	**X**	
CBP-IT-08-53	Out of Date and Inaccurate ACS Security Administrator Procedures	**X**	
CBP-IT-08-54	ACE Access Control Weaknesses	**X**	
CBP-IT-08-55	NDC LAN Accounts Created by Unauthorized Parties	**X**	

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

APR 8 2010

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 FY 2009 CBP Financial Statement Audit

In response to the memorandum dated March 10, 2010 requesting written comments on the draft report, responses to its recommendations, and identification of information that should not be publicly released, CBP OIT is providing the following comments on the remediation actions that are being performed for the findings and recommendations from the FY 2009 audit.

General comments

CBP OIT concurs with the preface of the report and page 2 of the January 22, 2010 letter from OIG which states that this management letter is FOUO and is the restricted distribution version of the overall report.

Thirty NFRs were issued to CBP OIT during the FY 2009 audit (11 were reissues of FY 2008 findings and 19 were new). To date, remediation on 12 findings has been completed. Corrective Action Plans (CAPs) for the remaining are either under development or are in progress and their status is provided in the attachment.

Access Controls

CBP concurred with KPMG's 18 findings and recommendations in this area. Work on 12 findings has been completed and await review by the auditors. Four other CAPs are on track for completion this fiscal year. Plans have not yet been received for two of the findings. The status of each CAP is provided in the attachment.

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

Security Management

CBP concurred with KPMG's ten findings and recommendations in this area. Remediation work has been completed on one of the findings. The Offices of Administration, Internal Affairs and Information Technology are cooperating to remediate the other nine findings which are expected to be completed by the end of the fiscal year. The status for each CAP is provided in the attachment.

Segregation of Duties

CBP concurred with KPMG's finding and recommendation in this area. CBP will continue the collaboration between the ACE Security Team, the Office of Administration, and the Office of Field Operations to identify and document incompatible roles. CBP will then develop a procedure to ensure incompatible roles are not assigned to the same user, unless an exception is properly authorized. The estimated completion date is July 15, 2010.

After-Hours Physical Security and Social Engineering Testing

CBP concurred with KPMG's finding and recommendation in this area. The Office of Information Technology in conjunction with the Office of Internal Affairs and the Privacy Office is working to develop a plan to strengthen the security awareness programs for protecting electronic and physical data, hardware, and personally identifiable information, as well as information marked "For Official Use Only." The estimated completion date is October 13, 2010.

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

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2009

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Acting Deputy Commissioner, CBP
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, CBP
Chief Information Officer, CBP
Chief Information Security Officer
Assistant Secretary, Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
Audit Liaison, CBP

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.