Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2010 U.S. Customs and Border Protection Financial Statement Audit

(Redacted)

OIG-11-90

June 2011

Office of Inspector General

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

Homeland
Security

JUN 14 2011

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 2010 U.S. Customs and Border Protection (CBP) financial statement audit as of September 30, 2010. It contains observations and recommendations related to information technology internal controls that were summarized in the *Independent Auditors Report* dated January 25, 2011 and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at CBP in support of the DHS FY 2010 financial statement audit and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated January 31, 2011, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal controls or conclusions concerning 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 20036-3389

January 31, 2011

Office of Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Customs and Border Protection

Chief Financial Officer
U.S. Customs and Border Protection

Ladies and Gentlemen:

We have audited the consolidated balance sheets of the U.S. Customs and Border Protection (CBP), a Component of the U.S. Department of Homeland Security (DHS), as of September 30, 2010 and 2009, and the 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. 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 (FY) 2010 engagement, we considered CBP's internal control over financial reporting by obtaining an understanding of CBP's internal controls, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and the Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended. 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 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 material weakness is a deficiency, or 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. A significant deficiency is a deficiency, or 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.

Our audit of CBP as of, and for the year ended, September 30, 2010, disclosed a significant deficiency in the areas of Information Technology (IT) access controls, security management, segregation of duties, and functionality. These matters are described in the *IT General Control Findings and Recommendations* section of this letter.

The significant deficiency described above is presented in our *Independent Auditors' Report*, dated January 25, 2011. 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**.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. We aim to use our knowledge of 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 2010 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.

CBP's written response to our comments and recommendations included in Appendix D has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

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

Very truly yours,

KPMG LLP

Department of Homeland Security
Customs and Border Protection
Information Technology Management Letter
September 30, 2010

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	1
Summary of Findings and Recommendations	3
IT General Control Findings and Recommendations	4
Security Management	4
After-Hours Physical Security Testing	5
Social Engineering Testing	5
Access Control	6
Segregation of Duties	7
Financial System Functionality	7
Application Control Findings	11
Management's Comments and OIG Response	11

APPENDICES

Appendix	Subject	Page
A	Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit	12
B	FY 2010 Notices of IT Findings and Recommendations at CBP	15
	- Notice of Findings and Recommendations – Definition of Severity Ratings	16
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at CBP	32
D	Management's Comments	34

Department of Homeland Security
Customs and Border Protection
Information Technology Management Letter
September 30, 2010

OBJECTIVE, SCOPE, AND APPROACH

We have audited the CBP agency's balance sheets and related consolidated statements of net cost, changes in net position, and custodial activity, and the combined statements of budgetary resources (hereinafter, referred to as "consolidated financial statements") as of September 30, 2010 and 2009. In connection with our audit of CBP's consolidated financial statements, we performed an evaluation of information technology general controls (ITGC), to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is further 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 five 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 or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.
- *Segregation of Duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
- *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 procedures, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls in the CBP environment. The technical security testing was performed both over the Internet and from within select CBP facilities, and focused on test, development, and production devices that directly support key general support systems.

In addition to testing CBP's general control environment, we performed application control tests on a limited number of CBP's 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. FISCAM defines application controls as follows: Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

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

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2010, CBP took corrective action to address prior year IT control weaknesses. For example, CBP made improvements over various system logical access processes and system security settings, system administrator access processes and procedures, and performed more consistent tracking of contractors and system user rules of behavior agreements. However, during FY 2010, we continued to identify IT general control weaknesses that could potentially impact CBP's financial data. 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 considered 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 2010 audit of the CBP consolidated financial statements. In addition, based upon the results of our test work, we noted that CBP did not fully comply with the requirements of the FFMIA.

In FY 2010, our IT audit work identified 23 IT findings, of which 16 were repeat findings from the prior year and 7 were new findings. In addition, we determined that CBP remediated 13 IT findings identified in previous years. Collectively, these findings represent deficiencies in three of the five FISCAM key control areas as well as deficiencies related to financial system functionality. The FISCAM areas impacted included Security Management, Access Controls, and Segregation of Duties. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and CBP financial data could be exploited thereby compromising the integrity of financial data used by management and reported in CBP's financial statements.

The recommendations made by us in this report are intended to be helpful, and may not fully remediate the deficiency. CBP management has responsibility to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

IT GENERAL CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2010 CBP financial statement audit, we identified the following IT and financial system control deficiencies that in the aggregate are considered a significant deficiency:

Security Management

- A complete, up-to-date listing of all CBP workstations is not maintained. As a result, CBP cannot determine whether CBP workstations are adequately protected against security threats.

- Of the forty-five selected employees that had separated in FY 2010, 19 of these individuals did not have a completed CBP Form 241 on file.

- Separation procedures relating to CBP contractors refer to Department of Treasury policies, and therefore are outdated as CBP is no longer a part of Treasury. Additionally, CBP-242 contractor separation forms were not properly completed for 9 of 45 selected CBP contractors.

- Non-Disclosure Agreements (NDAs) for 29 of 45 selected contractors were signed several months after their hire date, were not signed and/or dated by the contractor, and/or were not completed by CBP.

- CBP has not completed reinvestigations of contractors that should have been completed during the FY 2010 fiscal year (previous investigation date was greater than five years).

- During technical testing, access, configuration and patch management exceptions were identified on Active Directory (AD) Domain Controllers and hosts supporting the SAP, the Automated Commercial System (ACS), and the Automated Commercial Environment (ACE) applications.

- Role-based security training requirements for personnel with IT security positions were inadequate and were not commensurate with the individual's duties and responsibilities. Additionally, 8 of the 45 sampled individuals did not complete the required specialized training by the CBP deadline.

- Access to the raised floor area at the National Data Center (NDC) was not consistently documented by approved access requests. Additionally, not all personnel with access to the raised floor area were re-authorized for access.

After-Hours Physical Security Testing

After-hours physical security testing was conducted 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 hosting financial information. The testing was performed at various CBP locations that process and /or maintain financial data as shown in the following table.

Exceptions Noted	CBP Locations Tested						Total Exceptions by Type
	NDC-7 (BLM Building)	NDC-1	Beauregard (Alexandria)	Falls Church	Tyson's Corner	NDC-4	
Passwords	1	1	2	2	6	4	**16**
For Official Use Only (FOUO)	5	18	5	5	6	4	**43**
Keys/Badges	3	1	0	6	1	2	**13**
Personally Identifiable Information (PII)	4	4	0	1	0	2	**11**
Server Names/IP Addresses	1	5	1	0	2	1	**10**
Laptops	0	3	0	0	1	2	**6**
External Drives	0	0	1	1	0	0	**2**
Credit Cards	1	0	0	0	0	0	**1**
Total Exceptions by Location	**15**	**32**	**9**	**15**	**16**	**15**	**102**

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 for gaining computer system access.

Total Called	Total Answered	Number of People Who Divulged a Password
25	16	2

Access Control

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

- The following issues exist in regard to ACS Security Profile Change Log Procedures:
  - Procedures do not define how often the ACS security profile change audit logs are reviewed;
  - Procedures do not describe how evidence of the review process is created by the ACS Information System Security Officer (ISSO)/Independent Reviewer; and,
  - Procedures do not define the sampling methodology that is used to select ACS profile change security logs for review.

- ACE audit logs are not being reviewed on a regular basis.

- The control option to limit the number of failed logon attempts to the [redacted] was not configured properly.

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

- Initial access requests and approvals for 9 of 25 individuals granted access to ACE during FY 2010 could not be provided.

- ACE portal accounts for [redacted] are not timely removed as required by CBP and DHS policy.

- Access request documentation for individuals who had their ACS access profiles modified during FY 2010 was not consistently maintained.

- Activities of developers granted temporary/emergency access to ACS production were not monitored for appropriateness.

- Access request documentation for individuals who were granted access to the NDC Local Area Network (LAN) during FY 2010 was not consistently maintained.

- Personnel with access to backup media maintained off site have not regularly been recertified to validate the need for continuing access and the specific levels of access warranted.

Segregation of Duties

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

Financial System Functionality

KPMG identified control weaknesses related to the processing of drawback payments and in certain entry processes, which are reported in detail in the *Independent Auditors' Report.* These weaknesses are reported here in the Information Technology Management Letter to emphasize the common technology link within these findings as related to ACS.

ACS is used to track, control, and process commercial goods and conveyances for the purpose of collecting import duties, fees, and taxes owed to the Federal government and processing refunds and drawbacks related to the process of these collections. Since ACS was created in the mid-1980s, maintenance for the system has become increasingly difficult and expensive. Furthermore, the funding necessary to substantially remediate these control weaknesses is not available.

These control weaknesses continue to exist where ACS is functionally deficient. The conditions below highlight the deficiencies within ACS.

- ACS lacks the controls necessary to prevent, or detect and correct excessive drawback claims. The programming logic in ACS does not link drawback claims to imports at a detailed, line item level. In addition, ACS does not have the capability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries and export documentation upon which the drawback claim is based. Export information is not linked to the Drawback module and therefore electronic comparisons of export data cannot be performed within ACS.

- Certain monitoring reports used to monitor (review) importer compliance with the in-bond process have not been developed and therefore importer compliance is not being tracked. In addition, in-bonds are not automatically linked to the relevant entry or export filings in ACS, which leads to extensive manual work to close open in-bonds. Finally, ACS does not provide the ability to run oversight reports to determine if ports have completed all required in-bond post audits and exams.

- ACS does not properly account for bond sufficiency of claims that involve a continuous bond and therefore a claimant can potentially claim and receive an accelerated payment that exceeds the bond amount on file. As a result, CBP will not have sufficient surety against a drawback over claiming.

- ACS does not provide summary information of the total unpaid assessments for duties, taxes, and fees by individual importer (i.e., a sub-ledger) and cannot provide reporting information on outstanding receivables, the age of receivables, or other data necessary for management to effectively monitor collection actions.

- The drawback selectivity function of ACS is not programmed to select a statistically valid sample of prior drawback claims against a selected import entry.

- ACS is programmed to automatically indicate that a Port Director certified a refund or drawback payment even if the Port Director does not certify a given payment.

Recommendations:

We recommend that the CBP Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer**,** make the following improvements to CBP's financial management systems and associated information technology security program.

<u>For Security Management</u>

- Continue installing [redacted] and develop, implement, and monitor policies and procedures to move all workstations to [redacted] or to obtain waivers and compensating controls for those workstations that cannot be moved to [redacted].

- Review the validity of the CBP Form 241 for the Employee Separation process and to originate an alternate mechanism to hold managers accountable for timely notification of employee separations and for confirming the termination of access to information systems, and the return of Government property and equipment;

- Review the current Customs Directive and update it to reflect the current operating environment. Additionally, consistent and accurate completion of the SF Form 242 is required for all separating contractors with access to CBP facilities, information systems and/or sensitive information;

- Implement a more consistent method of ensuring that each contractor employee in moderate and high-risk positions complete and sign a NDA;

- Additional work:
  - Complete via e-QIP the "initiation" of all remaining employee reinvestigations by December 30, 2010.
  - Complete the reinvestigations for all such employees by December 30, 2011.
  - Develop/deploy a tracking mechanism (Contractor Tracking System) by which to identify those contractors requiring reinvestigation;

- Develop and implement a strategy to ensure that reinvestigations for all contractors are initiated as required;

- Patch, upgrade, correct, or obtain waivers for any identified weaknesses as a result of the IT technical vulnerabilities assessment;

- Re-examine the CBP role-based training program and consider implementing the DHS Role-Based Security Training Program at CBP once it is implemented at DHS; and

- Develop tools and procedures for facilitating and documenting the approval/recertification and review of individual access to the raised floor area.

For After-Hours Physical Security Testing:

- Implement multiple types of security awareness reminders and opportunities to educate users of the importance of protecting CBP information systems and data. Specifically, social engineering evaluations should be incorporated into routine site inspections to test employee security awareness and to educate users on how to respond to information security attacks.

For Social Engineering Testing:

- Continue annual security awareness training. In addition, seek to add other means of increasing security awareness.

<u>For Access Control</u>

- Formalize a detailed procedure for the review of ACS security profile change logs. The procedure should include implementing a periodic review of the logs by an independent reviewer**;**

- Develop and implement procedures that document the review process for ACS profile change logs. The process should include the documented evidence of review, how often audit logs are reviewed, and the review sampling methodology to be used;

- Maintain evidence that regular reviews of audit logs are occurring. Specifically, continue plans initiated in July of 2010 to institutionalize a more formal method of documenting who performed reviews of audit logs, when these reviews occurred, and what issues (if any) were identified. ;

- Perform a cost/benefit analysis to determine whether an ACE custom-developed solution or a purchased commercial off the shelf (COTS) product should be implemented for full automation of audit log reviews;

- Devote sufficient resources in order to implement and maintain formal ISAs with the Partnering Government Agencies (PGAs) that interconnect with ACS. Document ISAs for all ACS PGA connections identified in the ACS SSP;

- Issue a memorandum and distribute the procedures to the respective CBP Offices to implement monitoring procedures to ensure compliance with stated procedures and that Office Information Technology (OIT) coordinate a meeting with the other CBP Offices to determine if centralized access control measures are necessary;

- Implement procedures to reinforce adherence to guidance requiring timely notification of separations by employees or contractors with access to ACE. Those responsible for ACE access control need to be notified of a separation no later than the day of separation;

- Implement and monitor procedures to consistently document the access requests and approvals for any and all access creations and changes to ACS user profiles;

- For the TSS audit of emergency access, run a report, as needed, at management's (e.g., emergency approver's) request;

- Transition the process for requesting NDC-LAN Network access from the paper-based user access request form to an electronic user access request form. Once the electronic form is fully implemented, update the documented process to reflect that all NDC-LAN user access requests must go to the Technology Service Desk (TSD) for action. TSD will generate a trouble ticket and attach the electronic access request form to the initial user request ticket for NDC-LAN access. The ticket will be issued in the name of the user gaining the access so it is easily searchable; and

- Update the access authorization process to indicate that the access list will undergo a 100% recertification annually. The artifact derived from this action should be an official report from the Contracting Officer Technical Representative for offsite media storage clearly stating the recertification results along with the backup paperwork for all adds, deletes, and changes to the access list.

<u>For Segregation of Duties</u>

- Continue to work with the Office of International Trade, Office of Administration and Office of Field Operations to identify incompatible roles and develop procedures as part of the access control process to ensure that these role combinations are not granted to ACE users, except when a waiver is granted in writing.

<u>Lack of Financial System Functionality</u>

- Continue efforts on the following:
  - Modernize business processes though the development and deployment of functionality in the Automated Commercial Environment as it has done since 2001.
  - Work with ACE stakeholders, including CBP personnel, the trade, participating government agencies, the Department of Homeland Security and the Congress to prioritize, develop, and deploy functionality that allows CBP to fulfill its mission and meet the needs of its stakeholders.
  - Seek funds through the budget process that will allow CBP to continue to develop and deploy functionality in ACE that will support CBP's mission and meet the needs of its stakeholders.

APPLICATION CONTROL FINDINGS

We did not identify any findings in the area of application controls during the fiscal year 2010 CBP audit engagement.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from CBP 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

Appendix A

Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit

Department of Homeland Security
Customs and Border Protection
Information Technology Management Letter
September 30, 2010

Below is a description of significant CBP financial management systems and supporting IT infrastructure included in the scope of CBP's FY 2010 Financial Statement Audit.

Automated Commercial Environment (ACE)

ACE is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. It is CBP's plan that this system will replace ACS when ACE is fully implemented. The mission of ACE is to implement a secure, integrated, government-wide system for the electronic collection, use, and dissemination of international trade and transportation data essential to Federal agencies. ACE is being deployed in phases, with no set final full deployment date due to funding setbacks. As ACE is partially implemented now and processes a significant amount of revenue for CBP, ACE was included in full scope in the FY2010 financial statement audit. The ACE system is located in Newington, VA.

Automated Commercial System (ACS)

ACS is a collection of mainframe-based business process systems used to track, control, and process commercial goods and conveyances entering the United States territory, for the purpose of collecting import duties, fees, and taxes owed to the Federal government. ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations and illegal imports. The ACS system is included in full scope in the FY 2010 financial statement audit. The ACS system is located in Newington, VA.

National Data Center – Local Area Network (NDC LAN)

The NDC LAN provides more than 1,200 CBP contractor and employee user access to enterprise-wide applications and systems. The mission of the NDC LAN is to the support Field Offices/Agents with applications and technologies in the securing and protection of our nation's borders. The NDC LAN consists of five Novell NetWare 6.5 servers, various workstations and printers/plotters, 11 Cisco switches, and the associated Novell Netware management applications. There are no major or minor applications running on the NDC LAN other than the file and print services associated with the Novell NetWare servers. The NDC LAN is an unclassified system processing For Official Use Only (FOUO) data. As the NDC LAN includes the environment where the ACE, ACS, and SAP applications physically reside, the NDC LAN is included in limited scope in the FY2010 financial statement audit. The NDC LAN is located in Newington, VA.

SAP Enterprise Central Component (SAP ECC 6.0)

SAP is a client/server-based financial management system and includes the Funds Management, Budget Control System, General Ledger, Real Estate, Property, Internal Orders, Sales and Distribution, Special Purpose Ledger, and Accounts Payable modules. These modules are used by CBP to manage assets (e.g., budget, logistics, procurement, and related policy), revenue (e.g., accounting and commercial operations: trade, tariff, and law enforcement), and to provide information for strategic decision making. The SAP ECC 6.0 financial management system is included in full scope in the FY 2010 financial statement audit. The SAP ECC 6.0 system is located in Newington, VA.

Appendix B

FY 2010 Notices of IT Findings and Recommendations at CBP

Department of Homeland Security
Customs and Border Protection
Information Technology Management Letter
September 30, 2010

Notice 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 DHS Consolidated 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 prioritizing the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
Customs and Border Protection
Information Technology Management Letter
September 30, 2010

FY 2010 Information Technology
Notification of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-10-01	This is a system-level finding. KPMG noted that CBP portal accounts for [redacted] 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. KPMG did note that CBP is aware of the issue and is looking into an automated solution for compliance with CBP and DHS policy. Upon further testing of terminated employees, KPMG did not find any users that had accessed the system after their separation date from CBP.	CBP should implement procedures to reinforce adherence to guidance requiring timely notification of separations by employees or contractors with access to ACE. Those responsible for ACE access control need to be notified of a separation no later than the day of separation.		X	2
CBP-IT-10-02	This is a system level finding. KPMG noted that ACE is not currently configured to prevent incompatible roles from being assigned to a user, as required by CBP and DHS policies. While, initial steps have been taken to address formal segregation of duties within the system, no additional actions have taken place.	CBP Office of Information and Technology will continue to work with the Office of International Trade, Office of Administration and Office of Field Operations to identify incompatible roles and develop procedures as part of the access control process to ensure that these role combinations are not granted to ACE users, except when a waiver is granted in writing.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-10-03	This is a system-level finding. KPMG noted that evidence of completed ACE system log (Syslog) reviews did not include an appropriate level of detail. Specifically, during the majority of FY2010, there was no formal method of documenting who performed the audit log reviews, when they were reviewed, what issues (if any) were identified, and the actions taken (if applicable). KPMG noted that procedures regarding the review of ACE audit logs have been established prior to fiscal year 2010, and that management is currently implementing a formal method of documenting the requisite system log review information.	We recommend that CBP maintain evidence that regular reviews of audit logs are occurring. Specifically, we recommend that CBP continue with plans initiated in July of 2010 to institutionalize a more formal method of documenting who performed reviews of audit logs, when these reviews occurred, and what issues (if any) were identified. We also recommend that CBP perform a cost/benefit analysis to determine whether an ACE custom-developed solution or a purchased COTS product should be implemented for full automation of audit log reviews.		X	2
CBP-IT-10-05	Social engineering is defined as the act of attempting to manipulate or deceive people into taking action that is inconsistent with policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or computer system access.	We recommend that CBP implement multiple types of security awareness reminders and opportunities to educate	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	The objective of our social engineering test work primarily focused on attempting to identify user passwords. Posing as DHS technical support employees, attempts were made to obtain this type of account information by contacting randomly selected employees by telephone. A script was used to ask for assistance from the user in resolving a network issue in the component. For each person we attempted to call, we noted in the table below whether the individual answered and whether we obtained any information from them that should not have been shared with us according to DHS policy. Our selection of individuals was not statistically derived, and therefore we are unable to project results to the component or department as a whole. Of 25 individuals called, 16 answered. Of the 16 that answered, 2 divulged their network password.	users of the importance of protecting CBP information systems and data. Specifically, we recommend that social engineering evaluations be incorporated into routine site inspections to test employee's security awareness and to educate users on how to respond to information security attacks.			
CBP-IT-10-06	This is a system-level finding. KPMG requested access authorization documentation for 25 individuals who were granted ACE access during FY 2010. Initial access requests and approvals for 9 of these individuals were not provided. Although a process for creating and maintaining user access forms and requests has been in place since before the beginning of FY 2010, access approvals prior to the creation of ACE accounts were not consistently maintained in accordance with CBP policy and procedures.	We recommend that the Office of Information and Technology (OIT) issue a memorandum and distribute the procedures to the respective CBP Offices to implement. We also recommend that monitoring procedures be established to ensure compliance with the procedures and that OIT coordinate a meeting with the other CBP Offices to determine if centralized access control measures are		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		necessary.			
CBP-IT-10-07	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 equipment that houses financial data and information residing on CBP personnel desks, which could be used by others to inappropriately access financial information. The testing was performed at various CBP locations that process and/or maintain financial data. A CBP employee was designated to assist with and monitor our test work. After gaining access to CBP facilities, we inspected a selection of desks and/or offices, looking for items such as improper protection of system passwords, unsecured information system hardware, documentation marked “For Official Use Only” (FOUO), and unlocked network sessions. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. For each location visited, we note the type of unsecured information or property we identified and included the total exceptions noted by location, as well as by type of information or property identified. A total of 102 instances were identified across the six locations where physical assets or sensitive information was not secured in accordance with DHS and/or CBP policies.	CBP should continue its annual security awareness training. In addition, it should seek to add other means of increasing security awareness.		X	2
CBP-IT-10-08	This is a component-level finding. KPMG noted that separation procedures for contract employees (Customs Directive 51715-006) are out of date and include incomplete and inaccurate references. Specifically, the procedures have not been updated since September 2001. The procedures reference Treasury facilities and Treasury policies as source documentation. KPMG notes that a new directive, CBP Directive 1210-007, entitled ‘Contractor Tracking System,’ was issued requiring the use of the Contractor Tracking System; however, the new directive still refers to out of date Customs Directive 51715-006 for separation procedures	We recommend that CBP review the current Customs Directive and update it to reflect the current operating environment. Additionally, we recommend that CBP require the consistent and		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	for contractor employees. Additionally, KPMG noted that SF 242 contractor separation forms are not completed consistently for separating CBP contractors. Specifically, KPMG noted that of 45 separated contractors with access to CBP facilities, information systems, and/or sensitive information who were selected for testing, 9 forms were not completed, were not provided, or were not completed in a timely manner.	accurate completion of the SF 242 for all separating contractors with access to CBP facilities, information systems and/or sensitive information.			
CBP-IT-10-09	This is a component level finding. KPMG selected 45 government employees that had separated in FY 2010 and noted that 19 of these individuals did not have a completed CBP Form 241 on file.	We recommend that CBP review the validity of the CBP Form 241 Employee Separation process and determine an alternate mechanism to hold managers accountable for timely notification of employee separations and for confirming the termination of access to information systems, and the return of property and equipment.		X	2
CBP-IT-10-10	This is a component level finding. While KPMG notes that progress has been made in implementing procedures requiring the signing of NDAs, KPMG noted that NDAs are still not consistently completed by contractors at CBP. Specifically, KPMG noted that out of a selection of 45 contractors, one NDA was signed more than four months after the hire date. In addition, one NDA was not provided for a contractor in a medium or high risk position. Further, KPMG	We recommend that CBP implement a more consistent method of ensuring that each contractor employee in moderate and high-risk		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	noted that the NDAs for 27 contractors in medium or high risk positions did not have a date of signature.	positions sign and date a NDA.			
CBP-IT-10-11	This is a component-level finding. KPMG has noted that CBP has not been able to provide evidence that workstations not on [redacted] are receiving anti-virus and other security patch updates on a timely basis. 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 has not been maintained for the majority of FY 2010. As a result, CBP does not have an accurate inventory of which workstations have not received anti-virus and other security patch updates.	We recommend that CBP continue installing [redacted] and develop, implement, and monitor policies and procedures to move all workstations to [redacted] or to obtain waivers and compensating controls for those workstations that cannot be moved to [redacted].		X	2
CBP-IT-10-12	CBP's Role Based Security Training Program does not meet the DHS requirements for "annual specialized training" that is "commensurate with the individual's duties and responsibilities." Specifically, the CBP RBST program requires IT personnel to complete only one hour of Incident Response training, and one hour of Classified Information training (if applicable to the individual's responsibilities) annually. Furthermore, out of the sampled 45 CBP personnel with significant IT security responsibilities, 5 completed the training after CBP's internal June 30, 2010 deadline. In addition, another eight have yet to complete the training.	We recommend that CBP re-examine its role-based training program and consider implementing the DHS RBST Program once it has been implemented at the department level.	X		2
CBP-IT-10-13	This is a component-level finding. We noted the following weaknesses related to access to the raised floor area: • We reviewed access request authorizations to the raised floor area of [redacted] and noted that of the 45 individuals selected, 1 authorized access form was	We recommend that management develop tools and procedures for facilitating and documenting the	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	not provided. • We reviewed evidence of the recertification of individuals with access to the raised floor area and noted that of the 15 selected individuals, 2 had not yet been recertified.	approval/recertification and review of individual access to the raised floor area.			
CBP-IT-10-14	This is a system level finding. KPMG noted that although changes to a user's ACS access profile are logged, the logs of these events are not regularly reviewed by personnel independent from those individuals that made the changes.	We recommend that CBP formalize a detailed procedure for the review of ACS security profile change logs. The procedure should include implementing a periodic review of the logs by an independent reviewer.		X	2
CBP-IT-10-15	During our technical testing, patch and configuration management exceptions were identified on the [redacted]	We recommend that CBP perform the following remedial actions: 1 [redacted]	X		2

Department of Homeland Security
Customs and Border Protection
Information Technology Management Letter
September 30, 2010

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted].	3 [redacted].			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		9 [redacted]			
CBP-IT-10-16	This is a system-level finding and a prior year issue from FY2008 and FY2009. KPMG determined that evidence of ISAs for 6 of the 17 PGAs identified in the System Security Plan could not be provided. Of the six that were provided, two expired during FY2010 and had not been renewed.	We recommend that CBP devote sufficient resources in order to implement and maintain formal ISAs with the PGAs that interconnect with ACS. We recommend that CBP document ISAs for all ACS PGA connections identified in the ACS SSP.		X	2
CBP-IT-10-17	This is a system-level finding. We requested access authorization evidence for 45 ACS users to determine whether ACS access was appropriately authorized. OIT was unable to provide evidence of the access request authorizations for any of the 45 selected ACS users. As a result, we are not able to determine whether ACS access initiations or modifications were appropriately approved and whether ACS access controls are in place and operating as required by DHS and CBP policies.	We recommend that CBP implement procedures to consistently document the access requests and approvals for any and all access creations and changes to ACS user profiles.		X	2
CBP-IT-10-18	This is a component level finding. We noted that access request forms, or evidence of recertification of access, to the offsite media could not be provided for 5 of the 15 selected employees.	We recommend that CBP update the access authorization process to indicate that the access list will undergo a 100% recertification annually.	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		The artifact should be an official report from the Contracting Officer Technical Representative for offsite media storage clearly stating the results along with backup paperwork for all add, deletes, and changes to the access list.			
CBP-IT-10-19	This is a system level finding. We were informed that ACS Security Audit Logs are not being reviewed. Additionally, we noted that the following weaknesses related to the ACS Security Audit Logs procedures continue to exist: • Procedures do not define how often the ACS security profile change audit logs are reviewed. • Procedures do not describe how the documented evidence of the review process is created by the ACS (ISSO)/Independent Reviewer. • Procedures do not define the sampling methodology that is used to select ACS profile change security logs for review	We recommend that CBP develop and implement procedures that document the review process for ACS profile change logs. The process should include the documented evidence of review, how often audit logs are reviewed, and the review sampling methodology.		X	2
CBP-IT-10-20	This is a system-level finding. We noted the following weaknesses related to the [redacted] configuration settings: • KPMG noted that users were allowed an [redacted] number of failed attempts to access datasets to which they were not authorized. 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, had not been configured properly. KPMG noted that this setting was corrected on February 24, 2010.	As the conditions were closed during testing, no recommendation is required.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• KPMG noted that users were allowed failed logon attempts before their accounts were locked. At the end of the fiscal year the setting was updated to three failed login attempts, and KPMG observed the setting in the system and noted that it was corrected on September 24, 2010.				
CBP-IT-10-21	This is a component level finding. We noted the following weaknesses related to the CBP Background Investigation process: • Of the 45 individuals selected, we noted that 1 contractor did not have a completed background investigation as required by the CBP Information System Security Policies and Procedures Handbook. We noted that this contract has access to the ACE system. • Of the 45 individuals selected, we noted that 5 employees and 25 contractors did not have their background reinvestigations initiated within the five year timeframe as required by CBP Memorandum Regarding Reinvestigations, dated August 18, 2008.	KPMG recommends that CBP: • Complete via e-QIP the "initiation" of all remaining employee reinvestigations by December 30, 2010. • Complete the reinvestigations for all such employees by December 30, 2011. • Develop/deploy a tracking mechanism (Contractor Tracking System) by which to identify those contractors requiring reinvestigation. • Develop and implement a strategy to ensure that reinvestigations for all contractors are initiated as required.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-10-22	This is a system-level finding. ACS developers may gain emergency/temporary access to the production environment through the portal request process. While the emergency/temporary account activities are logged, CBP does not review these activity logs to identify inappropriate activities.	KPMG recommends that CBP reports on the TSS audit of emergency access should be run as needed at management's (e.g., emergency approver's) request.	X		2
CBP-IT-10-23	This is a system-level finding. Access approvals prior to the creation of NDC-LAN accounts were not consistently maintained in accordance with CBP policy and procedures. KPMG requested access authorization documentation for 25 individuals who were granted NDC-LAN access during FY 2010. Although a process for creating and maintaining user access forms and requests has been in place since before the beginning of FY 2010, initial access requests and approvals for 10 of these individuals were not provided.	We recommend that CBP fully transition their process for requesting NDC-LAN Network access from the paper-based user access request form to an electronic user access request form. Once the electronic form is fully implemented, the documented process will be updated to reflect that all NDC-LAN user access requests must go to the Technology Service Desk (TSD) for action. TSD will generate a trouble ticket and attach the electronic access request form to the initial user request ticket for NDC-LAN access. The ticket will be issued in the name of the user gaining	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		the access so it is easily searchable. TSD is currently in the development phase for a new user account request portal which will provide a secure online environment for managing this process. This new tool will allow requestors the ability to complete and submit LAN and eMail account requests via online web form. Once the request is reviewed and approved by the CBP supervisor, a ticket will be automatically generated (bypassing the need of saving/attaching and emailing the TSD) and routed to the appropriate group for processing. A log will be captured and saved in the new system for each approved/denied request for future reference.			
CBP-IT-10-	CBP has not corrected functionality issues currently noted in ACS, and routine maintenance is increasingly difficult and expensive. Currently, only two vendors	To address this finding,	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
24	support ACS, which limits CBP's ability to obtain maintenance services at a reasonable cost. During FY 2010, CBP spent nearly $12.1 million just to maintain ACS at its current level of functionality. In addition, CBP is currently re-visiting the amount of funding necessary to complete the implementation of the ACE financial modules and will complete this analysis in FY 2011. Due to these conditions regarding the functionality of ACS and delayed implementation of ACE, CBP has not resolved the following known ACS functionality issues: • ACS lacks the controls necessary to prevent, or detect and correct excessive drawback claims. The programming logic in ACS does not link drawback claims to imports at a detailed, line item level. In addition, ACS does not have the capability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries and export documentation upon which the drawback claim is based. Export information is not linked to the Drawback module and therefore electronic comparisons of export data cannot be performed within ACS. See NFR **CBP-10-20** for further details. • Certain monitoring reports used to monitor (review) importer compliance with the in-bond process have not been developed and therefore importer compliance is not being tracked. In addition, in-bonds are not automatically linked to the relevant entry or export filings in ACS, which leads to extensive manual work to close open in-bonds. Finally, ACS does not provide the ability to run oversight reports to determine if ports have completed all required in-bond post audits and exams. See NFR **CBP-10-14** for further details. • ACS does not properly account for bond sufficiency of claims that involve a continuous bond and therefore a claimant can potentially claim and receive an accelerated payment that exceeds the bond amount on file. As a result, CBP will not have sufficient surety against a drawback over claiming. See	CBP recommends that it continue to: 1. Modernize its business processes though the development and deployment of functionality in the Automated Commercial Environment as it has done since 2001. 2. Work with stakeholders, including CBP personnel, the trade, participating government agencies, the Department of Homeland Security and the Congress to prioritize, develop, and deploy functionality that allows CBP to fulfill its mission and meet the needs of its stakeholders. 3. Seek funds through the budget process that will allow CBP to continue to develop			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	NFR **CBP-10-05** for further details. • ACS does not provide summary information of the total unpaid assessments for duties, taxes, and fees by individual importer (i.e., a sub-ledger) and cannot provide reporting information on outstanding receivables, the age of receivables, or other data necessary for management to effectively monitor collection actions. See NFR **CBP-10-04** for further details. • The drawback selectivity function of ACS is not programmed to select a statistically valid sample of prior drawback claims against a selected import entry. See NFR **CBP-10-03** for further details. • ACS is programmed to automatically indicate that a Port Director certified a refund or drawback payment even if the Port Director does not certify a given payment. See NFR **CBP-10-19** for further details.	and deploy functionality in that will support CBP's mission and meet the needs of its stakeholders.			

APPENDIX C

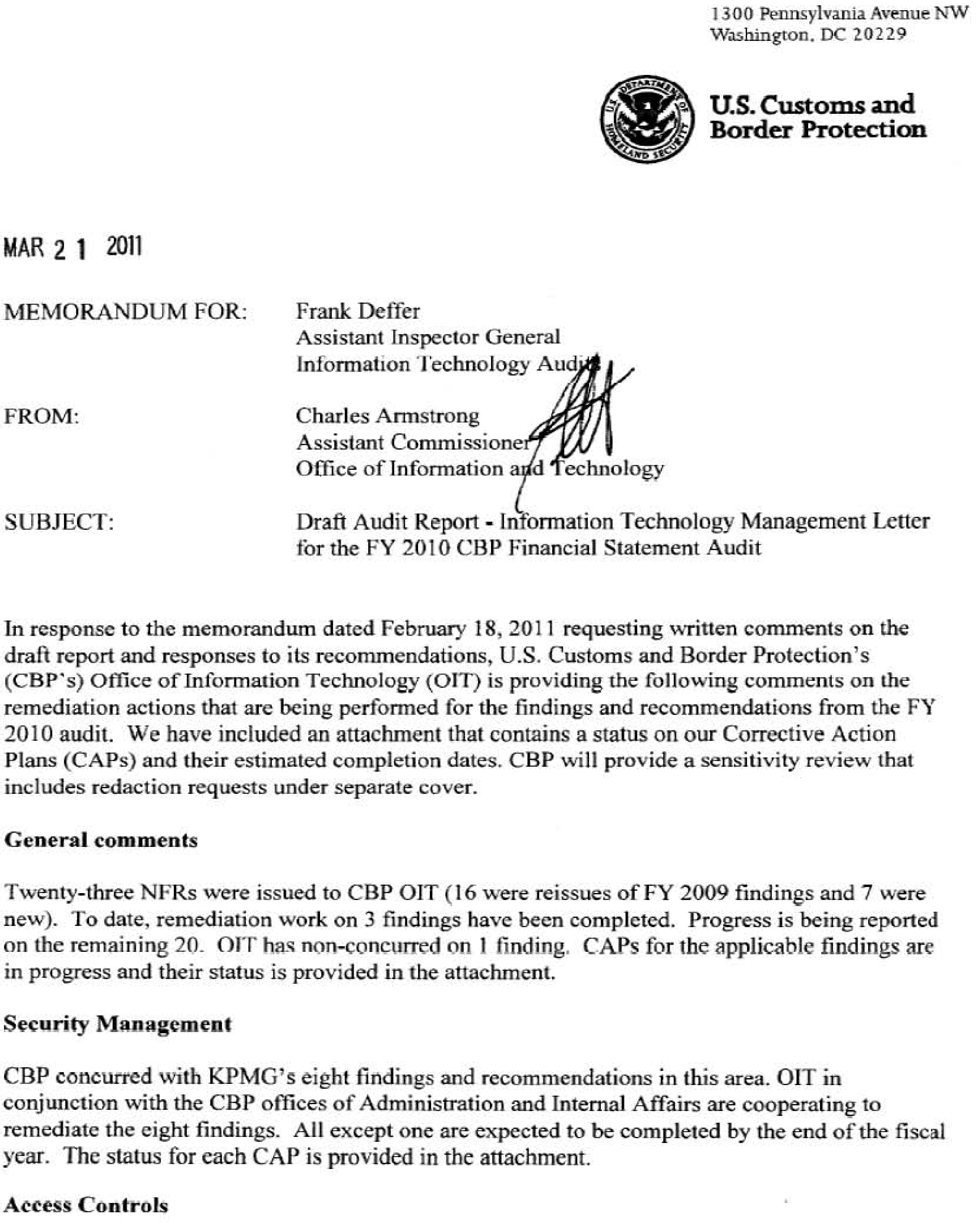
Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at CBP

Department of Homeland Security
Customs and Border Protection

Information Technology Management Letter

September 30, 2010

NFR No.	Description	Disposition	
		Closed	Repeat
CBP-IT-09-03	Contractor Tracking Deficiencies	X	
CBP-IT-09-12	[redacted] Install		CBP-IT-10-11
CBP-IT-09-13	Complete List of CBP Workstations		CBP-IT-10-11
CBP-IT-09-21	Review of Changes to Security Profiles in ACS		CBP-IT-10-14
CBP-IT-09-27	[redacted] Administrator Access Authorization Weaknesses	X	
CBP-IT-09-29	Completion of CF-241 Forms for Terminated Employees		CBP-IT-10-09
CBP-IT-09-34	Installation of Anti-Virus Protection		CBP-IT-10-11
CBP-IT-09-41	Weaknesses in the Process of Separating CBP Contractors		CBP-IT-10-08
CBP-IT-09-44	Completion of Non Disclosure Agreements for US CBP Contractors		CBP-IT-10-10
CBP-IT-09-45	Log configuration weakness for [redacted] System.	X	
CBP-IT-09-48	Lack of Effective ACS Access Change Log Review Procedures		CBP-IT-10-19
CBP-IT-09-56	ACE Audit Log Reviews		CBP-IT-10-03
CBP-IT-09-57	NDC LAN Audit Logs	X	
CBP-IT-09-58	Novell Password Settings	X	
CBP-IT-09-59	Formal Procedures for Mainframe System Utility Logs	X	
CBP-IT-09-60	Configuration for Mainframe Security Violation Control Option		CBP-IT-10-20
CBP-IT-09-61	Completion of Initial Background Investigations and Periodic Background Reinvestigations for CBP Employees and Contractors		CBP-IT-10-21
CBP-IT-09-62	Rules of Behavior Not Consistently Signed by CBP Employees and Contractors	X	
CBP-IT-09-63	ACE does not disable accounts after 45 days	X	
CBP-IT-09-64	ACS PGA ISAs Not Completely Documented		CBP-IT-10-16
CBP-IT-09-65	Documentation of ACE Access Change Requests		CBP-IT-10-06
CBP-IT-09-66	Separated Employees on ACE Access Listing		CBP-IT-10-01
CBP-IT-09-67	Inadequate Documentation of ACS Access Change Requests		CBP-IT-10-17
CBP-IT-09-68	Vulnerabilities in Configuration and Patch Management	X	
CBP-IT-09-69	Inadequate SAP Profile Change Review	X	
CBP-IT-09-70	Overuse of ACS Emergency/Temporary Access Roles	X	
CBP-IT-09-71	Inadequate Documentation of SAP Emergency/Temporary Access Requests	X	
CBP-IT-09-72	ACE Segregation of Duties Controls are Not In Place		CBP-IT-10-02
CBP-IT-09-73	Inadequate Documentation of ACE SCO Access Requests and Approvals	X	
CBP-IT-09-74	Inadequate Protection of CBP Information and Property		CBP-IT-10-05 CBP-IT-10-07



1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and
Border Protection

MAR 2 1 2011

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 2010 CBP Financial Statement Audit

In response to the memorandum dated February 18, 2011 requesting written comments on the draft report and responses to its recommendations, U.S. Customs and Border Protection's (CBP's) Office of Information Technology (OIT) is providing the following comments on the remediation actions that are being performed for the findings and recommendations from the FY 2010 audit. We have included an attachment that contains a status on our Corrective Action Plans (CAPs) and their estimated completion dates. CBP will provide a sensitivity review that includes redaction requests under separate cover.

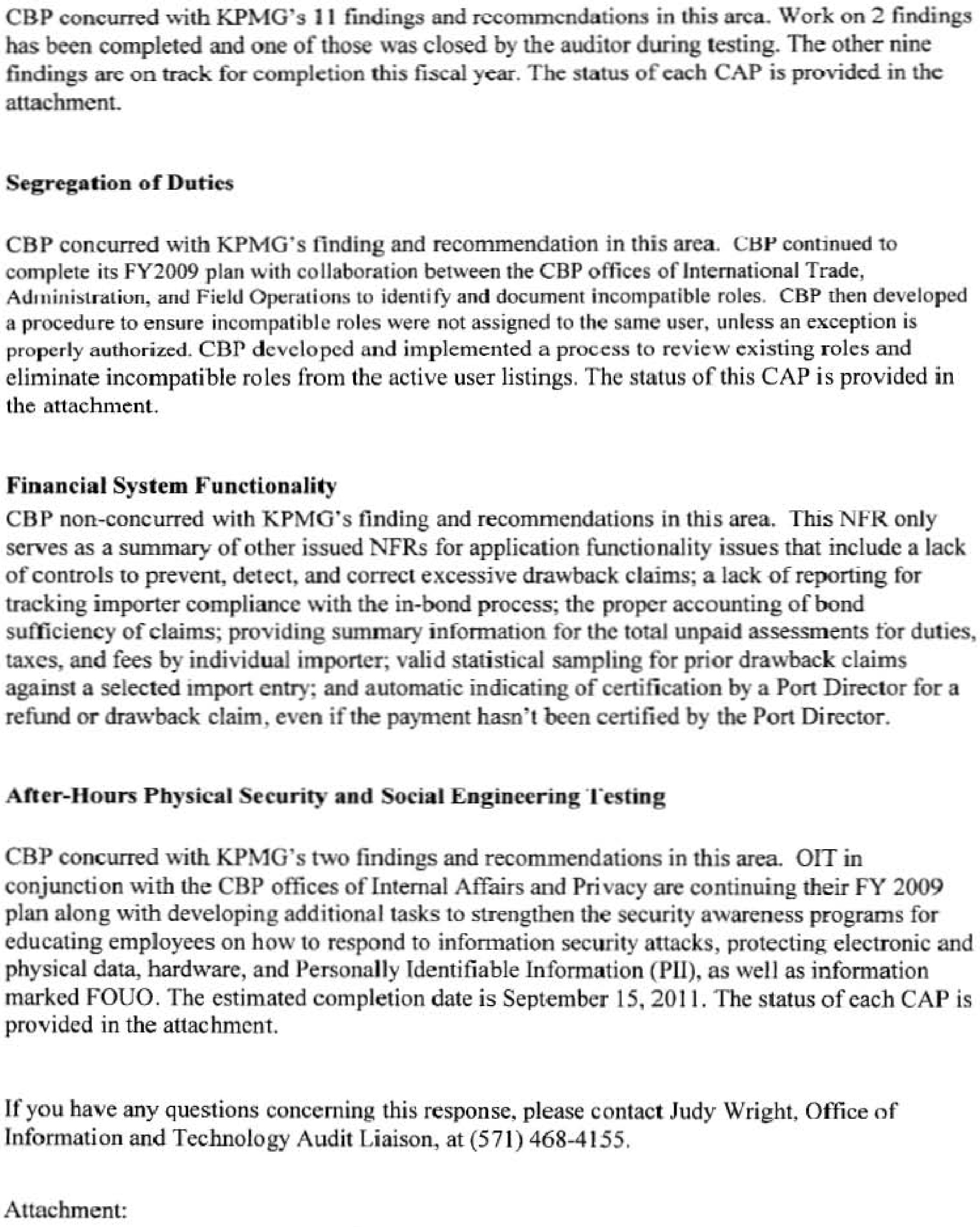
General comments

Twenty-three NFRs were issued to CBP OIT (16 were reissues of FY 2009 findings and 7 were new). To date, remediation work on 3 findings have been completed. Progress is being reported on the remaining 20. OIT has non-concurred on 1 finding. CAPs for the applicable findings are in progress and their status is provided in the attachment.

Security Management

CBP concurred with KPMG's eight findings and recommendations in this area. OIT in conjunction with the CBP offices of Administration and Internal Affairs are cooperating to remediate the eight findings. All except one are expected to be completed by the end of the fiscal year. The status for each CAP is provided in the attachment.

Access Controls



CBP concurred with KPMG's 11 findings and recommendations in this area. Work on 2 findings has been completed and one of those was closed by the auditor during testing. The other nine findings are on track for completion this fiscal year. The status of each CAP is provided in the attachment.

Segregation of Duties

CBP concurred with KPMG's finding and recommendation in this area. CBP continued to complete its FY2009 plan with collaboration between the CBP offices of International Trade, Administration, and Field Operations to identify and document incompatible roles. CBP then developed a procedure to ensure incompatible roles were not assigned to the same user, unless an exception is properly authorized. CBP developed and implemented a process to review existing roles and eliminate incompatible roles from the active user listings. The status of this CAP is provided in the attachment.

Financial System Functionality

CBP non-concurred with KPMG's finding and recommendations in this area. This NFR only serves as a summary of other issued NFRs for application functionality issues that include a lack of controls to prevent, detect, and correct excessive drawback claims; a lack of reporting for tracking importer compliance with the in-bond process; the proper accounting of bond sufficiency of claims; providing summary information for the total unpaid assessments for duties, taxes, and fees by individual importer; valid statistical sampling for prior drawback claims against a selected import entry; and automatic indicating of certification by a Port Director for a refund or drawback claim, even if the payment hasn't been certified by the Port Director.

After-Hours Physical Security and Social Engineering Testing

CBP concurred with KPMG's two findings and recommendations in this area. OIT in conjunction with the CBP offices of Internal Affairs and Privacy are continuing their FY 2009 plan along with developing additional tasks to strengthen the security awareness programs for educating employees on how to respond to information security attacks, protecting electronic and physical data, hardware, and Personally Identifiable Information (PII), as well as information marked FOUO. The estimated completion date is September 15, 2011. The status of each CAP is provided in the attachment.

If you have any questions concerning this response, please contact Judy Wright, Office of Information and Technology Audit Liaison, at (571) 468-4155.

Attachment:

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 for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of 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.