Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the FY 2011 U.S. Customs and Border Protection Financial Statement Audit

OIG-12-77

May 2012

Office of Inspector General

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

May 1, 2012

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 2011 U.S. Customs and Border Protection (CBP) Component financial statement audit as of September 30, 2011. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors' Report* dated January 27, 2012 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at the CBP component in support of the DHS FY 2011 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter 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
Office of Information Technology Audits

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

March 28, 2012

Acting Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
U.S. Customs and Border Protection

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, 2011 and 2010, and the 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") 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) 2011 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*. 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, 2011, disclosed a significant deficiency in the areas of Information Technology (IT) security management, access controls, configuration management, segregation of duties, contingency planning, and application controls. These matters are described in the *General IT Control Findings and Recommendations* and the *Application Control Finding and Recommendation* sections of this letter.

The significant deficiency described above is presented in our *Independent Auditors' Report*, dated January 27, 2012. This letter represents the separate restricted distribution letter mentioned in that report.

KPMG LLP is a Delaware limited liability partnership, the U.S. member firm of KPMG International Cooperative ("KPMG International"), a Swiss entity.

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 2011 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.

This communication is intended solely for the information and use of DHS and CBP management, the DHS Office of Inspector General (OIG), the OMB, the 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.

Very truly yours,

KPMG LLP

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

Department of Homeland Security
U.S Customs and Border Protection
Information Technology Management Letter
September 30, 2011

OBJECTIVE, SCOPE, AND APPROACH

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), 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, 2011 and 2010. In connection with our audit of CBP's consolidated financial statements, we performed an evaluation of general information technology controls (GITCs), to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A.

FISCAM was designed to inform financial auditors about information technology (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 provide reasonable assurance that security management is effective.
- *Access Control (AC)* – Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals.
- *Configuration Management (CM)* – Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended.
- *Segregation of Duties (SD)* – Controls provide reasonable assurance that incompatible duties are effectively segregated.
- *Contingency Planning (CP)* – Controls provide reasonable assurance that contingency planning: (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions 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 from within select CBP facilities, and focused on production devices that directly support key general support systems.

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

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2011, 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. However, during FY 2011, we identified new and continuing general IT 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. The IT findings were combined into a significant deficiency regarding IT for the FY 2011 audit of the CBP consolidated financial statements.

In FY 2011, our IT audit work identified 36 IT findings, of which 19 were repeat findings from the prior year and 17 were new findings. In addition, we determined that CBP remediated 4 IT findings identified in previous years. Collectively, these findings represent deficiencies in all five FISCAM key control areas, as well as deficiencies related to financial system functionality. 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 related deficiency. CBP management has the responsibility to determine the most appropriate methods for addressing the weaknesses identified based on their system capabilities and available resources.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2011 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

- Systems certification and accreditation:
  - System security plan updates were not current or effectively communicated for one system;
  - Security test and evaluation documentation was not completed annually for multiple systems, in accordance with DHS policy; and
  - Interconnection security agreements (ISA) were not fully documented for one system.
- Non-current policies and procedures:
  - Separation procedures for contract employees were out of date and included incomplete and inaccurate references.
- Lack of compliance with existing policies:
  - IT-based specialized security training requirements had not been fully implemented and enforced;
  - Several instances where background investigations of federal employees and contractors employed to operate, manage and provide security over IT systems were not being properly conducted;
  - Non-disclosure agreements were not consistently completed;
  - Exit processing procedures for transferred/terminated personnel, including contractors, were not consistently followed or communicated internally in a timely manner; and
  - Evidence on whether CBP workstations that are not currently part of the Microsoft Active Directory are being managed to receive current security patches could not be provided.

After-Hours Physical Security Testing

During the after-hours physical security walkthrough of selected CBP locations in the Washington, D.C. area, 18 instances were identified where assets and information with inadequate protection against unauthorized access, misuse, or misappropriation. Specific weaknesses identified and the locations where the instances were identified are included in the following matrix:

Exceptions Noted	CBP Locations Tested					Total Exceptions by Type
	NDC-7 (BLM Building)	NDC-1	Beauregard (Alexandria)	Tyson's Corner	National Place	
Passwords	0	2	0	0	2	**4**
For Official Use Only (FOUO)	0	2	0	0	0	**2**
Keys/Badges	0	0	0	0	0	**0**
Personally Identifiable Information (PII)	1	5	0	0	1	**7**
Server Names/IP Addresses	1	1	0	0	0	**2**
External Drives, Removable Media, Blackberries, or Other Unsecured Property	1	0	0	0	1	**2**
Credit Card Numbers	1	0	0	0	0	**1**
Classified Documents	0	0	0	0	0	**0**
Total Exceptions by Location	**4**	**10**	**0**	**0**	**4**	**18**

Note that approximately 15 desks / offices were examined at each of the locations above.

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, shown in the following table:

Total Called	Total Answered	Number of people who provided a username and/or password
36	25	1 – Both User Name and Password

Access Control

- Deficiencies in management of application and/or database accounts, network, and remote user accounts:
  - Strong password requirements were not enforced for network accounts;
  - User account lists were not periodically reviewed for appropriateness, and users were not disabled or removed promptly upon personnel termination; and
  - Initial access and modified access granted to application and/or database, network, and remote users were not properly documented and authorized.
- Ineffective or insufficient use of available audit logs:
  - Logs of auditable events were not being reviewed to identify potential incidents, or were reviewed by those with conflicting roles; and
  - Documented procedures for audit log follow-up did not meet DHS requirements.

Configuration Management

- Lack of documented policies and procedures:
  - Configuration, vulnerability, and patch management plans had not been established and implemented, or did not comply with DHS policy.
- Security patch management and configuration deficiencies were identified during the vulnerability assessment on hosts supporting the key financial applications and general support systems.

Segregation of Duties

- Lack of evidence to show that least privilege and segregation of duties controls exist for one system; and
- Users with privileged access were granted conflicting roles which compromised segregation of duties principles. Further, mitigating controls were not in place to identify unauthorized activities performed by individuals with conflicting access roles.

Contingency Planning

- One system's contingency plan was not updated based on recent testing results; and
- Access to backup media was not regularly reviewed and updated based on changes to personnel staffing and job roles.

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.

Security Management

- Update systems security policies and procedures to be in compliance with DHS policy.
- Maintain and update and system security plans and other relevant system documentation to reflect current conditions and results of testing and control reviews.
- Maintain current ISAs for in-scope applications, and maintain a current listing of these interconnections.
- Maintain, update, and communicate personnel hiring and termination policies. In addition, enforce the implementation of internal controls for the personnel processes including the completion of non-disclosure agreements.
- Complete all investigations and periodic reinvestigations of personnel as required by DHS policy during fiscal year 2012.
- Continue with the development and testing of a Role-Based Security Training (RBST) pilot program based on the DHS RBST program model.
- Develop a process to ensure workstations are properly updated with security patches.

After-Hours Physical Security Testing:

- Continue efforts to enhance the CBP security awareness campaigns.

Social Engineering Testing:

- Implement multiple types of security awareness reminders and opportunities to educate users on the importance of protecting CBP information systems and data.

Access Control

- Implement and configure technology to record user account changes. In addition, implement a process to regularly and independently reconcile changes made to user accounts within the application to source authorization documentation.

- Ensure that all requests for general and emergency access to applications, systems, and networks, including remote users, are supported by an appropriately authorized request for access. Conduct training for security administrators as necessary to ensure compliance with this process.

- Recertify, revalidate, and update privileged and non-privileged user access.

- Revoke user access in a timely manner when personnel are transferred, separated from the organization, or when job duties change and no longer necessitate a need for system access.

- Implement a process for logging changes to critical and sensitive data and regularly reviewing the contents of these logs. Maintain evidence of the review of these logs.

- Implement controls to enforce password complexity requirements including protecting against the use of passwords that contain dictionary-based words.

Configuration Management

- Finalize and formally distribute an updated configuration management plan.

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

Segregation of Duties

- Identify system and application roles that should not be combined based on the principles of segregation of duties. When segregation of duties are compromised based on a valid business reason, perform and document independent reviews of activities executed by users with non-segregated access.

Contingency Planning

- Maintain current contingency plans for the in-scope systems that reflect current conditions and the results of testing the contingency plans.

- Periodically recertify personnel with access to backup media stored off site. Maintain documentation of this recertification of access.

APPLICATION CONTROL FINDING AND RECOMMENDATION

During the FY 2011 CBP financial statement audit, we identified the following application control and financial system functionality deficiency that, when aggregated with the GITC deficiencies, is considered a significant deficiency:

Finding:

- One financial system lacks the controls necessary to prevent, or detect and correct excessive drawback claims. Specifically, the programming logic for the system does not link drawback claims to imports at a detailed, line item level. This would potentially allow the importer to receive claims in excess of an allowable amount.

Recommendation:

- We recommend that the CBP CIO and CFO, in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer prioritize, develop, and deploy functionality that will allow CBP to prevent or detect and correct excessive drawback claims.

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

Appendix A

Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2011 DHS Financial Statement Audit

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

Below is a description of significant U.S. Customs and Border Protection (CBP) financial management systems and supporting IT infrastructure included in the scope of CBP's FY 2011 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, without a 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 FY 2011 financial statement audit. The ACE system is located in Virginia (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 was included in full scope in the FY 2011 financial statement audit. The ACS system is located in VA.

National Data Center – Local Area Network (NDC LAN)

The NDC-LAN was absorbed by the DC Metro LAN and the Data Center Infrastructure LAN during the end of FY 2011. The NDC-LAN provided more than 1,200 CBP contractor and employee user's access to enterprise-wide applications and systems. The mission of the NDC-LAN was to the support Field Offices/Agents with applications and technologies in the securing and protection of our nation's borders. The NDC-LAN consisted of five Novell NetWare 6.5 servers, various workstations and printers/plotters, 11 Cisco switches, and the associated Novell Netware management applications. There were 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 was an unclassified system processing For Official Use Only (FOUO) data. As the NDC-LAN included the environment where the ACE, ACS, and SAP applications physically reside, the NDC-LAN was included in limited scope in the FY 2011 financial statement audit. The NDC LAN is located in VA.

Systems, Applications, and Products, Enterprise Central Component (SAP ECC)

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 financial management system was included in full scope in the FY 2011 financial statement audit. The SAP ECC system is located in VA.

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

Appendix B

FY 2011 Notices of IT Findings and Recommendations at CBP

Appendix B

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

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 CBP 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 reporting purposes.

These ratings are provided only to assist CBP in prioritizing 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, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
CBP-IT-11-01	Security Awareness Issued Identified During Enhanced Security Testing	Access Controls	2		X
CBP-IT-11-02	Physical Security Issues Identified During Enhanced Security Testing	Access Controls	2		X
CBP-IT-11-03	Inadequate Role-based Security Training Program	Security Management	2		X
CBP-IT-11-04	Segregation of Duties Control Weaknesses Within a CBP System	Access Controls	3		X
CBP-IT-11-05	CBP System User Profile Change Logs are Not Reviewed	Access Controls	3		X
CBP-IT-11-07	Lack of Monitoring of Developer Emergency/Temporary Access to CBP System Production	Access Controls	3		X
CBP-IT-11-08	CBP System Novell Server Audit Logs Review Weaknesses	Access Controls	2	X	
CBP-IT-11-09	CBP System Contingency Plan Has Not Been Updated	Contingency Planning	1	X	
CBP-IT-11-10	Lack of Update to CBP System Security Plan	Security Management	2	X	
CBP-IT-11-11	Incomplete Background Investigations and Reinvestigations for CBP Employees and Contractors	Security Management	2		X
CBP-IT-11-12	Contractor Separation Procedures Were Not Updated and Contractor Separation Forms are Not Maintained	Access Controls	2		X
CBP-IT-11-13	Inadequate Documentation of CBP System Access Change Requests	Access Controls	2		X
CBP-IT-11-14	CBP System User Profile Change Logs Are Not Reviewed	Access Controls	3	X	
CBP-IT-11-15	Incomplete Access Request Forms and Approvals for New CBP System Accounts	Access Controls	3		X
CBP-IT-11-16	Lack of Annual Recertification of CBP System Users	Access Controls	3	X	
CBP-IT-11-17	Incomplete Access Request Approval Forms for New Remote Access User Accounts	Access Controls	2	X	

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
CBP-IT-11-18	Incomplete Documentation of Interconnection Security Agreements for CBP System Connections	Access Controls	2		X
CBP-IT-11-19	Contractor Non-Disclosure Agreements are Incomplete	Access Controls	2		X
CBP-IT-11-20	Weaknesses Over the Employee Separation Process	Access Controls	2		X
CBP-IT-11-21	CBP System Audit Logs Not Appropriately Reviewed	Access Controls	3	X	
CBP-IT-11-22	Lack of Access Requests and Approvals for CBP System Accounts	Access Controls	3		X
CBP-IT-11-23	Lack of Update to CBP System Security Test & Evaluation (ST&E)	Security Management	2	X	
CBP-IT-11-24	CBP System Configuration Management Policies and Procedures Not Formally Documented	Configuration Management	2	X	
CBP-IT-11-25	Weaknesses in Allowed Network Authenticators	Access Controls	2	X	
CBP-IT-11-26	CBP System Audit Logs Review Weaknesses	Access Controls	3		X
CBP-IT-11-27	Security Weaknesses Identified During the Technical Vulnerability Assessment	Security Management	2		X
CBP-IT-11-28	Security Posture of CBP Workstations	Security Management	2		X
CBP-IT-11-30	Separated Personnel on CBP System User Listing	Access Controls	3	X	
CBP-IT-11-31	Lack of Functionality in a CBP System	Application Controls	3		X
CBP-IT-11-32	Separated Personnel with Active Access Privileges to CBP System	Access Controls	2	X	
CBP-IT-11-33	Lack of Update to CBP System ST&E	Security Management	2	X	
CBP-IT-11-34	Lack of Update to CBP System ST&E	Security Management	2	X	
CBP-IT-11-35	Access to Media Recertification is Incomplete	Contingency Planning	1		X
CBP-IT-11-36	Lack of Annual Recertification of CBP System Users	Access Controls	3	X	

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
CBP-IT-11-37	CBP System Privileged User Access Weaknesses	Access Controls	3	X	
CBP-IT-11-38	CBP System Segregation of Duties Weaknesses over the Production Environment	Access Controls	3	X	

Note 1: NFRs numbers CBP-IT-11-06 and CBP-IT-11-29 were not used in this sequence.

Note 2: Specific system names were replaced with "CBP System" for security purposes

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

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
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2011

NFR #	Description	Disposition	
		Closed	Repeat
CBP-IT-10-01	Separated Employees on System User Listings	X	
CBP-IT-10-02	Segregation of Duties Control Weaknesses Within a CBP System		CBP-IT-11-04
CBP-IT-10-03	CBP System Audit Log Reviews are Not Formally Documented to Include All Appropriate Information and Detail		CBP-IT-11-26
CBP-IT-10-04	Recertification Review of CBP System User Accounts	X	
CBP-IT-10-05	Security Awareness Issue Identified During Enhanced Security Testing		CBP-IT-11-01
CBP-IT-10-06	Incomplete Access Request Forms and Approvals For New CBP System Accounts		CBP-IT-11-15
CBP-IT-10-07	Physical Security Issues Identified During Enhanced Security Testing		CBP-IT-11-02
CBP-IT-10-08	Contractor Separation Procedures are Not Updated and Contractor Separation Forms are Not Maintained		CBP-IT-11-12
CBP-IT-10-09	Employee Separation Forms are not Maintained		CBP-IT-11-20
CBP-IT-10-10	Non-Disclosure Agreements for CBP Contractors in Moderate and High-level Risk Positions are Not Completed		CBP-IT-11-19
CBP-IT-10-11	Installation of Virus Protections on CBP Workstations		CBP-IT-11-28
CBP-IT-10-12	Inadequate Role-Based Security Training Program		CBP-IT-11-03
CBP-IT-10-13	Raised Floor Access Authorization Process Weaknesses	X	
CBP-IT-10-14	CBP System User Profile Change Logs are Not Reviewed		CBP-IT-11-05
CBP-IT-10-15	Vulnerability Assessment Weaknesses with CBP Systems		CBP-IT-11-27
CBP-IT-10-16	Incomplete Documentation of Interconnection Security Agreements (ISA) for CBP System Participating Government Agencies (PGA) Connections		CBP-IT-11-18
CBP-IT-10-17	Lack of Access Requests and Approval for CBP System Account		CBP-IT-11-22
CBP-IT-10-18	Evidence of Personnel Authorization to Access Backup Media Not Available		CBP-IT-11-35
CBP-IT-10-19	CBP System User Access Profile Change Log Review Procedures Have Not Been Implemented		CBP-IT-11-05
CBP-IT-10-20	Unauthorized Access Attempt Setting for the Mainframe Have Not Been Configured	X	
CBP-IT-10-21	Background Investigations and Reinvestigations for CBP Employees and Contractors are Not Completed		CBP-IT-11-11
CBP-IT-10-22	Lack of Monitoring of Developer Emergency/Temporary Access to CBP System Production		CBP-IT-11-07
CBP-IT-10-23	Lack of Access Requests and Approval for CBP System Accounts		CBP-IT-11-13
CBP-IT-10-24	CBP System Functionality Issues		CBP-IT-11-31

Note: Specific system names were replaced with "CBP System" for security purposes.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2011

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
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
CBP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

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