Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the FY 2012 U.S. Customs and Border Protection Financial Statement Audit

OIG-13-88 (Revised)

May 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 24, 2013

MEMORANDUM FOR: The Honorable Thomas S. Winkowski
Deputy Commissioner
Performing the duties of the Commissioner of CBP
U.S. Customs and Border Protection

FROM: Charles K. Edwards
Deputy Inspector General

SUBJECT: *Information Technology Management Letter for the FY 2012 U.S. Customs and Border Protection Financial Statement Audit-Revised*

Attached for your information is the revised version of the final report, *Information Technology Management Letter for the FY 2012 U.S. Customs and Border Protection Financial Statement Audit.* This report contains observations related to information technology internal control. The revision to the report included a corrected report title and a new Appendix D, which replaced Appendix A, Report Distribution.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Frank Deffer, Assistant Inspector General for Information Technology Audits, at (202) 254-4100.

Attachment

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

April 4, 2013

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, 2012, and 2011, 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 engagement 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) 2012 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 audit 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.

Our audit engagement of CBP as of, and for the year ended, September 30, 2012, 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 25, 2013. 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 Notices of Findings and Recommendations (NFRs), 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 2012 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 report is intended solely for the information and use of DHS management, DHS Office of Inspector General (OIG), U.S. OMB, U.S. 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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

We have audited the consolidated balance sheets of the U.S. CBP, a component of the U.S. 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, 2012, and 2011. In connection with our engagement to audit CBP's consolidated financial statements, we performed an evaluation of general Information Technology (IT) controls (GITCs), to assist in planning and performing our audit engagement. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the 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 statement 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 statement audit. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a Federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the GITCs and the IT 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 GITC 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 2012, CBP took corrective action to address prior year IT control weaknesses. For example, CBP made improvements in various system logical access processes and system security settings. However, during FY 2012, we identified new and continuing GITC weaknesses that could potentially impact CBP's financial data. The most significant weaknesses related to controls over access to programs and data, segregation of duties, and configuration management. 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 operations, 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 2012 audit of the CBP consolidated financial statements. In addition, based upon the results of our test work, we noted that CBP contributes to the DHS' non-compliance with the requirements of the *Federal Financial Management Improvement Act of 1996*.

In FY 2012, our IT audit work identified 46 IT findings, of which 21 were repeat findings from the prior year and 25 were new findings. In addition, we determined that CBP remediated 15 IT findings identified in the prior year. 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.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During our engagement to audit the FY 2012 CBP financial statements, we identified the following CBP GITC and financial system control deficiencies that in the aggregate are considered a significant deficiency at CBP and in the aggregate contribute to the IT material weakness at the Department level:

Security Management

- Systems Security Authorization :
  - Interconnection security agreements (ISA) were expired and not fully documented for multiple systems;
  - Several financial systems and general support systems were not properly certified and accredited, in compliance with DHS policy; and
  - Privacy Threshold Analyses and Privacy Impact Assessments, Risk Assessments and Security Assessment Reports were not updated or approved in compliance with DHS policy for multiple systems.
- System Security Plans (SSP) did not reflect the current system environment, to include a current listing of external system connections for multiple systems.
- Lack of compliance with existing policies:
  - IT-based specialized security training requirements had not been fully implemented and enforced;
  - Background reinvestigations of Federal employees and contractors employed to operate, manage and provide security over IT systems were not being properly conducted;
  - Non-disclosure agreements (NDAs) were not consistently completed; and
  - Exit processing procedures for transferred/terminated personnel, including contractors, were not consistently followed or communicated internally in a timely manner.

After-Hours Physical Security Testing

During the after-hours physical security walkthrough of selected CBP locations in the Washington, DC area, 104 instances were identified where assets and information were inadequately protected 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 [(1)]	**National Data Center (NDC) 1**	**NDC 2**	**Beauregard**	**Falls Church**	**National Place**	**Total Exceptions**
Passwords [(2)]	5	0	1	0	3	**9**
For Official Use Only	24	5	4	4	6	**43**
Keys	3	1	0	0	0	**4**
Personally Identifiable Information	1	1	1	1	7	**11**
Unlocked Laptop/Workstation	2[(4)]	1	0	0	1[(5)]	**4**
Server Names/Internet Protocol (IP) Addresses [(3)]	21	3	0	1	0	**25**
Credit Cards	0	0	0	0	2	**2**
Classified Documents	0	0	0	0	0	**0**
External Drives, Other Media, Blackberries, etc.	0	0	0	3	3	**6**
Total Exceptions at CBP	**56**	**11**	**6**	**9**	**22**	**104**

Notes:

(1) The number of offices and cubicles inspected does not equal the total number of exceptions identified, since one office/cubicle may have had multiple exceptions.

(2) Attempts to login to the systems with the identified passwords were not performed. However, we assumed that the identified passwords were valid passwords.

(3) The unit of measure for Server Names/IP Addresses exceptions is at the document level, rather than at the individual server name/IP addresses level. For example, if a document contained multiple IP addresses, only one exception was noted. Consequently, each noted exception may contain multiple instances of Server Names/IP Addresses. In addition, IP address findings were not differentiated between IP addresses within a network diagram vs. IP addresses not on a network diagram.

(4) One unattended laptop was observed to be unlocked and did not display a password-protected screensaver.

(5) One unattended workstation was observed to be unlocked and did not display a password-protected screensaver.

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

Access Control

- Ineffective safeguards over logical and physical access to sensitive facilities and resources:
  - The physical access management system does not generate complete and accurate listings of users with access to the location where systems are physically hosted;
- Deficiencies in management of application and/or database accounts, network, and remote user accounts:
  - User account lists and/or change logs were not periodically reviewed for appropriateness;
  - Excessive user access privileges were allowed for several systems, and users logical access to systems and data was not disabled or removed promptly upon personnel termination; and
  - The process for authorizing and managing access to component systems and networks, including virtual private network and other remote access, did not comply with DHS and CBP requirements.
- Ineffective or insufficient use of available audit logs:
  - Logs of auditable events were not being completed appropriately, were not reviewed to identify potential incidents, or were reviewed by those with conflicting roles; and
  - Shared user accounts exist on the database and actions are not explicitly traceable to the users who executed the action.

Configuration Management

- Security patch management and configuration deficiencies were identified during the vulnerability assessment on hosts supporting the key financial applications and general support systems.
- The process for documenting, authorizing, testing and migrating application software changes and implementing operating system and database patches into production did not comply with DHS and component requirements.

Segregation of Duties

- Lack of evidence to show that least privilege and segregation of duties controls exist for two systems.
- Lack of monitoring developer's emergency and temporary access to the production environment.

Contingency Planning

- Service continuity plans were not reviewed in compliance with DHS policy.

Recommendations:

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

Security Management

- Document and renew interconnection documents on a timely basis, and update SSPs to reflect current external system connections;
- Initiate all outstanding periodic reinvestigations by the end of the fiscal year 2012 as required by DHS policy;
- Reiterate NDA policy requirements to the Contracting Officer's Representatives (CORs). Validate the process for completing and filing NDAs and implement improvements to ensure NDAs are appropriately completed;
- Ensure all roles with significant information security responsibilities are identified and defined. Ensure all employee and contractor personnel possessing these roles participate in and receive the appropriate Role-based Security Training (RBST) on an annual basis. Monitor those positions to ensure all employees and contractors participate in and receive the appropriate RBST;
- Ensure that all security authorization documentation is updated and reviewed at the frequency required by DHS policy; and
- Issue reminders to Federal Supervisors and CORs on the Federal employee and contractor separation clearance process. Ensure that Human Resources has included separation clearance as part of any Federal Supervisor and COR reference guides.

After-Hours Physical Security Testing:

- Provide security awareness training to all CBP employees through multiple mediums each year. Continuously remind users to protect passwords, sensitive information, and CBP media. Continue efforts to enhance the CBP security awareness campaigns, and focus on desktop reviews.

Access Control

- Ensure that the physical access management system is updated with a complete and accurate listing of users with access to the raised floor. Update physical security procedures to include any changes to the physical access management process;

- Explore capabilities to extract data for instances where developers have been granted emergency access to production. If the capabilities exist, develop and implement a process to review these actions for appropriateness;
- Implement and configure technology to record user account changes, update and implement processes for identifying and reconciling changes to access privileges to source documentation, and ensure that reviews over changes to access privileges are performed as required by DHS policy;
- Update the configuration setting for disabling operating system user accounts after a period of inactivity;
- Evaluate and update the current processes for provisioning access and 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 periodic internal verification reviews and training to ensure that security administrators and supervisors are enforcing compliance with these processes;
- Evaluate and update the current annual recertification process to ensure that all privileged and non-privileged user access is recertified, revalidated, and updated as required;
- Evaluate and update system user separation processes to ensure the user access is revoked in a timely manner when personnel are transferred, separated from the organization, or when job duties change and the user no longer needs system access;
- Implement a process for logging changes to critical and sensitive data and regularly review the contents of these logs as required by DHS policy. Maintain evidence of the review of these logs; and
- Require each database administrator to authenticate to the database using unique identifiers rather than shared user identifiers.

Configuration Management

- Develop a central repository for all artifacts related to change requests to ensure that all change requests are appropriately authorized and tested from initiation to completion;
- Evaluate change management and patching processes to ensure compliance with DHS policies. Enforce a timely approval and implementation of standard and emergency application changes and operating system and database patches; and
- Review all patching processes to ensure compliance with DHS policy. Resolve all vulnerabilities noted in the IT technical vulnerability assessment scan results. Remove all software no longer utilized or not authorized for use from all identified systems.

Segregation of Duties

- Implement segregation of application user duties within the access management system; and
- Establish a regular review of audit logs for indications of inappropriate or unusual activity where duties cannot be adequately segregated due to operational factors.

Contingency Planning

- Ensure that all security authorization documentation, including contingency plans, is updated and reviewed on the frequency as required by DHS policy.

APPLICATION CONTROL FINDING AND RECOMMENDATION

During the FY 2012 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 payment in excess of an allowable amount.

Recommendation:

We recommend that the CBP CIO and CFO, in coordination with the DHS Office of Chief Information Officer and the DHS Office of the Chief Financial Officer continue to pursue alternative compensating or automated controls and measures that may ultimately remediate the risk of overpayment and identify the potential revenue loss exposure to CBP. These alternative internal controls over drawback claims may result in the capability to compare, verify, and track essential information on drawback claims and identify duplicate or excessive drawback claims.

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2012

Appendix A

Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2012 CBP Financial Statement Audit

Below is a description of significant U.S. Customs and Border Protection (CBP) financial management systems and supporting information technology (IT) infrastructure included in the scope of CBP's FY 2012 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 the Automated Commercial System (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 2012 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 2012 financial statement audit. The ACS system is located in VA.

National Data Center – DC Metro Local Area Network (DC Metro LAN)

The DC Metro LAN provides more than 10,000 CBP contractors and employee user's access to enterprise-wide applications and systems. The mission of the DC Metro LAN is to support the mission of CBP operational elements in the DC Metro LAN region of the organization. These tools include personal computers, laptop computers, printers and file/print servers which enable CBP officers and agents to interact with all other applications and systems in the CBP environment. There are 21 major applications supported by the DC Metro LAN, including ACE and ACS. As the DC Metro LAN included the environment where the ACE, ACS, and SAP applications physically reside, the DC Metro LAN was included in the FY 2012 financial statement audit. The DC Metro 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 2012 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, 2012

Appendix B
FY 2012 Notices of IT Findings and Recommendations

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2012

FY 2011 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-12-01	Physical Security Issues Identified During Enhanced Security Testing	Access Controls		X
CBP-IT-12-02	Inadequate Role-Based Security Training Program	Security Management		X
CBP-IT-12-03	Segregation of Duties Control Weaknesses within CBP System	Access Controls		X
CBP-IT-12-04	CBP System User Profile Change Logs are not Reviewed	Access Controls		X
CBP-IT-12-05	CBP System User Profile Change Logs are not Reviewed	Access Controls		X
CBP-IT-12-06	Weaknesses in Creating New CBP System Accounts	Access Controls		X
CBP-IT-12-07	CBP System Audit Logs not Appropriately Reviewed	Access Controls		X
CBP-IT-12-08	Incomplete Background Re-Investigations for CBP Employees and Contractors	Security Management		X
CBP-IT-12-09	Contractor NDAs are Incomplete	Security Management		X
CBP-IT-12-10	Lack of Annual Recertification for CBP System Application Users	Access Controls	X	
CBP-IT-12-11	Incomplete Documentation of ISAs for CBP System Connections	Access Controls	X	
CBP-IT-12-12	Inadequate Documentation for CBP System Application Software Changes	Configuration Management	X	
CBP-IT-12-13	CBP System DB2 Database Patches are not Documented and Implemented Appropriately	Configuration Management	X	
CBP-IT-12-14	CBP System AIX Operating System Patches are not Implemented Appropriately	Configuration Management	X	
CBP-IT-12-15	CBP System Production and Training Operating Systems Vulnerability Scanning Process Weaknesses and Scan Results	Configuration Management		X
CBP-IT-12-16	Lack of Access Requests and Approvals for CBP System Accounts	Access Controls		X
CBP-IT-12-17	Lack of Monitoring Developer Emergency/Temporary Access to CBP System Production	Access Controls		X
CBP-IT-12-18	Lack of Annual Recertification for CBP System Privileged Users	Access Controls	X	

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2012

FY 2011 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-12-19	Incomplete Documentation of ISAs for CBP System Connections	Access Controls		X
CBP-IT-12-20	Inadequate Documentation for CBP System Application Software Changes	Configuration Management	X	
CBP-IT-12-21	CBP System LPARs and Linux z/OS Vulnerability Scanning Process Weaknesses and Scan Results	Configuration Management	X	
CBP-IT-12-22	CBP System Raised Floor Access Weaknesses	Access Controls	X	
CBP-IT-12-23	Lack of Functionality in the CBP System	Application Controls		X
CBP-IT-12-24	Inadequate Documentation of CBP System Access Requests	Access Controls		X
CBP-IT-12-25	Incomplete Access Request Approval Forms for New Remote Access User Account	Access Controls		X
CBP-IT-12-26	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-27	Separated Personnel on CBP System User Listing	Access Controls	X	
CBP-IT-12-28	Lack of Annual Recertification for CBP System Application, Oracle Database and Operating System Account Recertifications	Access Controls	X	
CBP-IT-12-29	CBP System Audit Logs are not Appropriately Reviewed	Access Controls	X	
CBP-IT-12-30	CBP System Technical Vulnerability Weaknesses	Configuration Management	X	
CBP-IT-12-31	Lack of Complete Review of CBP System Profile Changes	Access Controls	X	
CBP-IT-12-32	CBP System Vulnerability Scanning Process Weaknesses and Scan Results	Configuration Management	X	
CBP-IT-12-33	CBP System Configuration Setting for Disabling Inactive Accounts is not Configured Appropriately	Access Controls	X	
CBP-IT-12-34	Incomplete Documentation of ISAs for CBP System Connections	Access Controls	X	
CBP-IT-12-36	CBP System Oracle Database and Unix Operating Systems Patches are not Documented and Implemented Appropriately	Configuration Management	X	
CBP-IT-12-38	Employee Separation Process Weaknesses	Security Management		X

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2012

FY 2011 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-12-39	Contractor Separation Process Weaknesses	Security Management		X
CBP-IT-12-40	CBP System Segregation of Duties Weaknesses over the Production Environment	Configuration Management		X
CBP-IT-12-41	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-42	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-43	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-45	CBP System Program Library Access not Documented and Approved Appropriately.	Configuration Management	X	
CBP-IT-12-46	Separated Personnel on CBP System User Listing	Access Controls	X	
CBP-IT-12-47	Separated Personnel on CBP System User Listing	Access Controls		X
CBP-IT-12-48	Separated Personnel on CBP System Application and Operating System User Listing	Access Controls		X
CBP-IT-12-49	CBP System Audit Log Review Weaknesses	Access Controls	X	

Note 1: NFRs numbers CBP-IT-12-35, CBP-IT-12-37 and CBP-IT-12-44 were not used in this sequence.

Note 2: Specific system names were replaced with “CBP System” for security purposes.

Appendix C

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

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2012

NFR #	Description	Disposition	
		Closed	Repeat
CBP-IT-11-01	Security Awareness Issued Identified During Enhanced Security Testing	X	
CBP-IT-11-02	Physical Security Issues Identified during Enhanced Security Testing		X
CBP-IT-11-03	Inadequate Role-based Security Training Program		X
CBP-IT-11-04	Segregation of Duties Control Weaknesses within the CBP System		X
CBP-IT-11-05	CBP System User Access Profile Change Log Review Procedures Have Not Been Implemented		X
CBP-IT-11-07	Lack of Monitoring of Developer Emergency/Temporary Access to CBP System Production		X
CBP-IT-11-08	Lack of Monitoring of CBP System Novell Server Audit Logs	X	
CBP-IT-11-09	Lack of Update to CBP System Contingency Plan	X	
CBP-IT-11-10	Lack of Update to CBP System Security Plan	X	
CBP-IT-11-11	Background Investigations and Reinvestigations for CBP Employees and Contractors are not Completed		X
CBP-IT-11-12	Contractor Separation Procedures are not Updated and Contractor Separation forms are not Maintained		X
CBP-IT-11-13	Lack of Access Requests and Approval for CBP System Accounts		X
CBP-IT-11-14	CBP System Profile Change Logs are not Reviewed		X
CBP-IT-11-15	CBP System User Access Form Documentation is Incomplete		X
CBP-IT-11-16	CBP System Privileged User Recertification is Incomplete	X	
CBP-IT-11-17	Remote User Access Form Documentation is Incomplete		X
CBP-IT-11-18	CBP System Interconnection Security Agreements are Incomplete		X
CBP-IT-11-19	Contractor Non-Disclosure Agreement Weaknesses		X
CBP-IT-11-20	Employee Separations Weaknesses		X

Department of Homeland Security
U.S. Customs and Border Protection
Information Technology Management Letter
September 30, 2012

NFR #	Description	Disposition	
		Closed	Repeat
CBP-IT-11-21	CBP System Audit Log Review Weaknesses		X
CBP-IT-11-22	CBP System User Access Authorization Evidence Weakness		X
CBP-IT-11-23	CBP System Security Test & Evaluation Weakness	X	
CBP-IT-11-24	CBP System Configuration Management Policies and Procedures not Finalized	X	
CBP-IT-11-25	CBP System Account Authentication Weaknesses	X	
CBP-IT-11-26	CBP System Audit Log Review Weaknesses	X	
CBP-IT-11-27	Security Weaknesses Identified during Technical Vulnerability Assessment		X
CBP-IT-11-28	Security Posture of CBP Workstations	X	
CBP-IT-11-30	Separated Personnel on CBP System User Listings		X
CBP-IT-11-31	CBP System Functionality Issues		X
CBP-IT-11-32	CBP System User Account Termination Weaknesses		X
CBP-IT-11-33	CBP System Security Test & Evaluation Weakness	X	
CBP-IT-11-34	CBP System Security Test & Evaluation Weakness	X	
CBP-IT-11-35	Evidence of Personnel Authorization to Access Backup Media Not Available	X	
CBP-IT-11-36	CBP System Recertification Weaknesses	X	
CBP-IT-11-37	CBP System Privileged User Access Management Process Weaknesses	X	
CBP-IT-11-38	CBP System Privileged User Segregation of Duties Weaknesses		X

Note 1: NFRs numbers CBP-IT-11-06 and CBP-IT-11-29 were not used in the FY 2011 IT NFR sequence.

Note 2: Specific system names were replaced with “CBP System” for security purposes.

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Chief Financial Officer
Chief Information Officer
Chief Information Security Officer
Acting Chief Privacy Officer

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 document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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