

**OFFICE OF INSPECTOR GENERAL**

**Information Technology  
Management Letter For the FY  
2014 U.S. Customs and Border  
Protection Financial  
Statement Audit**



Homeland  
Security

**May 6, 2015  
OIG-15-60**



# HIGHLIGHTS

## *Information Technology Management Letter For the FY 2014 U.S. Customs and Border Protection Financial Statement Audit*

---

**May 6, 2015**

### **Why We Did This**

Each year, our independent auditors identify component-level information technology control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details that were not included in the fiscal year (FY) 2014 DHS Agency Financial Report.

### **What We Recommend**

We recommend that CBP, in coordination with the DHS Chief Information Officer and Chief Financial Officer, make improvements to its financial management systems and associated information technology security program.

#### **For Further Information:**

Contact our Office of Public Affairs at (202) 254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

### **What We Found**

We contracted with the independent public accounting firm KPMG LLP to perform the audit of the consolidated financial statements of U.S. Customs and Border Protection (CBP) and the Department of Homeland Security (DHS) for the year ended September 30, 2014. KPMG LLP evaluated selected general information technology controls, entity level controls, and business process application controls. KPMG LLP determined that CBP took corrective action by designing and consistently implementing certain account management controls.

However, KPMG LLP continued to identify deficiencies related to financial system functionality and general information technology controls regarding logical access and configuration management for CBP's core financial and feeder systems. Such control deficiencies limited CBP's ability to ensure the confidentiality, integrity, and availability of its critical financial and operational data.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

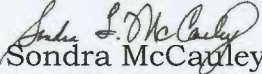
---

Washington, DC 20528

May 6, 2015

TO: Charles R. Armstrong  
Chief Information Officer  
U.S. Customs and Border Protection

Deborah Schilling  
Chief Financial Officer  
U.S. Customs and Border Protection

FROM:   
Sondra McCauley  
Assistant Inspector General  
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the FY 2014 U.S. Customs and Border Protection Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2014 U.S. Customs and Border Protection Financial Statement Audit*. This report contains comments and recommendations related to information technology internal control deficiencies. The observations did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2014, which was included in the FY 2014 DHS Agency Financial Report.

The independent public accounting firm KPMG LLP conducted the audit of DHS' FY 2014 financial statements and is responsible for the attached information technology management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control, nor do we provide conclusions on compliance with laws and regulations. We will post the final report on our website.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Division, at (202) 254-5451.

Attachment



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

December 19, 2014

Office of Inspector General,  
U.S. Department of Homeland Security, and  
Chief Information Officer and Chief Financial Officer,  
U.S. Customs and Border Protection,  
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Customs and Border Protection (CBP), a component of the U.S. Department of Homeland Security (DHS), as of and for the years ended September 30, 2014, and September 30, 2013 (hereinafter, referred to as the “fiscal year (FY) 2014 CBP consolidated financial statements”), in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, we considered CBP’s internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and OMB Bulletin No. 14-02. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers’ Financial Integrity Act* of 1982. Accordingly, we do not express an opinion on the effectiveness of CBP’s internal control.

During our audit we noted certain matters involving internal control and other operational matters at CBP that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies.

We identified certain internal control deficiencies at CBP during our audit that, in aggregate, represent a significant deficiency in information technology (IT) controls at CBP and, when combined with certain internal control deficiencies identified at certain other DHS Components, contribute to a material weakness in IT controls and financial system functionality at the DHS Department-wide level. Specifically, with respect to financial systems at CBP, we noted certain internal control deficiencies in the general IT control areas of security management, access controls, and configuration management, as well as in the area of business process application controls. These matters are described in the *Findings and Recommendations* section of this letter.

Additionally, at the request of the DHS Office of Inspector General (OIG), we performed additional non-technical information security procedures to identify instances where CBP



personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These matters are described in the *Observations Related to Non-Technical Information Security* section of this letter.

We have provided a description of key CBP financial systems and IT infrastructure within the scope of the FY 2014 CBP consolidated financial statement audit in Appendix A, and a listing of each CBP IT Notice of Finding and Recommendation communicated to management during our audit in Appendix B.

During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters at CBP, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the OIG and the CBP Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the FY 2014 CBP consolidated financial statements, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of CBP's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

**KPMG LLP**

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

**TABLE OF CONTENTS**

|  | <b>Page</b> |
|--|-------------|
| Objective, Scope, and Approach                             | 2           |
| Summary of Findings  | 4           |
| Findings and Recommendations                               | 6           |
| Findings   | 6           |
| Recommendations  | 7           |
| Observations Related to Non-Technical Information Security | 10          |

**APPENDICES**

| <b>Appendix</b> | <b>Subject</b>  | <b>Page</b> |
|-----------------|---|-------------|
| <b>A</b>        | Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2014 CBP Consolidated Financial Statement Audit | 12          |
| <b>B</b>        | FY 2014 IT Notices of Findings and Recommendations at CBP   | 15          |

## OBJECTIVE, SCOPE, AND APPROACH

### Objective

We audited the consolidated financial statements of the U.S. Customs and Border Protection (CBP), a component of the U.S. Department of Homeland Security (DHS), as of and for the years ended September 30, 2014, and September 30, 2013 (hereinafter, referred to as the “fiscal year (FY) 2014 CBP consolidated financial statements”). In connection with our audit of the FY 2014 CBP consolidated financial statements, we performed an evaluation of selected CBP general information technology (IT) controls (GITCs), IT entity-level controls (ELCs), and business process application controls (BPACs) to assist in planning and performing our audit engagement. At the request of the DHS Office of Inspector General (OIG), we also performed additional information security testing procedures to assess certain non-technical areas related to the protection of sensitive IT and financial information and assets.

### Scope and Approach

#### General Information Technology Controls and IT Entity-Level Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), formed the basis of our GITC and IT ELC evaluation procedures.

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, IT ELCs, and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs, IT ELCs, and the IT environment:

1. *Security Management* – 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.
2. *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
3. *Configuration Management* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.
4. *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
5. *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

While each of these five FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs and IT ELCs for evaluation based on their relationship to the ongoing effectiveness of process-level automated controls or manual controls with one or more automated components. This includes those controls which depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2014 GITC and IT ELC procedures at CBP did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

Where relevant GITCs were determined to be operating effectively, we performed testing over selected BPACs (process-level controls which were either fully automated or manual with an automated component) on financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions.

FISCAM defines BPACs as the automated and/or manual controls applied to business transaction flows and relate to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes.

Financial System Functionality

In recent years, we have noted that limitations in CBP's financial systems' functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs, IT ELCs, and BPACs supporting financial data processing and reporting. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2014, we continued to evaluate and consider the impact of financial system functionality on internal control over financial reporting.

Non-Technical Information Security Testing

To complement our IT controls test work, we conducted limited after-hours physical security testing and social engineering at selected CBP facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to CBP personnel awareness of policies, procedures, and other requirements governing the protection of sensitive IT and financial information and assets from unauthorized access or disclosure. This testing was performed in accordance with the FY 2014 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG, DHS OIG, and DHS management.

Appendix A provides a description of the key CBP financial systems and IT infrastructure within the scope of the FY 2014 CBP consolidated financial statement audit.



Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

## SUMMARY OF FINDINGS

During FY 2014, we noted that CBP took corrective action to address certain prior year IT control deficiencies. For example, CBP made improvements over designing and implementing certain account management controls. However, we continued to identify BPAC deficiencies related to financial system functionality, and GITC deficiencies related to controls over access controls (including, but not limited to, the generation and review of audit logs and the management of access to system components) and configuration management, for CBP core financial and feeder systems and associated General Support System (GSS) environments. In many cases, new control deficiencies reflected weaknesses over new systems in scope for FY 2014 which were remediated or historically effective in other system environments.

The conditions supporting our findings collectively 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, certain of these deficiencies at CBP adversely impacted the internal controls over CBP's and DHS' financial reporting and their operation, and we consider them to collectively represent a significant deficiency for CBP and to contribute to a Department-wide material weakness regarding IT controls and financial system functionality for DHS, under standards established by the American Institute of Certified Public Accountants and the U.S. GAO.

Of the 31 IT Notices of Findings and Recommendations (NFRs) issued during our FY 2014 testing, six were repeat findings, either partially or in whole from the prior year, and 25 were new findings. The 31 IT NFRs issued represent deficiencies and observations related to three out of the five FISCAM GITC categories, as well as in the area of BPACs.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with the requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and CBP policies and procedures, as applicable. The most significant weaknesses from a financial statement audit perspective continued to include:

1. Excessive, unauthorized, or inadequately monitored access to, and activity within, system components for key CBP financial applications;
2. Configuration management controls that were not fully defined, followed, or effective;
3. Lack of proper segregation of duties for roles and responsibilities within financial systems; and
4. System functionality limitations preventing adequate implementation of automated preventative or detective controls to support management and implementation of custodial revenue and drawback processes.

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we have noted that limitations in CBP's financial

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

systems' functionality may be inhibiting CBP's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Many key CBP financial systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and Office of Management and Budget (OMB) Circular Number A-123 Appendix D, *Compliance with FFMIA*.

While the recommendations made by us should be considered by CBP, it is the ultimate responsibility of CBP management to determine the most appropriate method(s) for addressing the deficiencies identified.

## FINDINGS AND RECOMMENDATIONS

### Findings

During our audit of the FY 2014 CBP consolidated financial statements, we identified the following GITC and IT ELC deficiencies, certain of which, in the aggregate, contribute to the IT significant deficiency at CBP and the IT material weakness at the Department level:

#### *Security Management*

- Security awareness training and role-based training for personnel with significant information security responsibilities was not consistently completed prior to granting system or network access or within required timeframes.
- Two interconnection security agreements (ISAs) had expired and one was not renewed in a timely manner.

#### *Access Controls*

- Account management activities on multiple financial system components (including the application, database, and operating system/mainframe layers) and the CBP network were not consistently or timely documented or implemented. These activities included authorization of new access, periodic recertification of access, and revocation of access from separated or transferred Federal employees and contractors.
- Generic, service, and group accounts on financial system databases were not properly controlled to limit the risk of unnecessary or unauthorized access.
- Administrator-level access within multiple system environments, including front-end user access with administrator privileges, was granted in conflict with the principles of least privilege and separation of duties, and was granted without the ability to trace individual activity due to the use of shared accounts.
- Account security controls, including inactivity lockout parameters, were not fully implemented for accounts on multiple financial system components.
- Audit logs for multiple financial system components (including the application, database, and operating system/mainframe layers) did not include all required auditable events at an adequate level of detail and were not consistently reviewed by management or retained, required annual reviews were not performed to verify the continued appropriateness of relevant security events subject to requirements for logging and periodic review, and logs were not adequately protected from unauthorized modification or deletion.

Department of Homeland Security  
*Information Technology Management Letter*  
U.S. Customs and Border Protection  
September 30, 2014

---

*Configuration Management*

- Controls to enforce segregation of duties between development and production migration activities during the configuration management lifecycle, establish individual accountability for activities performed within the production environment, and monitor records of such activity were inadequate.
- Password and remote access configuration deficiencies were identified during vulnerability assessments of system components supporting one financial application.
- Vulnerability management activities, including performing internal scans of financial applications and system software and implementing vendor-recommended patches to address known vulnerabilities, were not consistently performed.
- Audit procedures over certain controls and application functionality for one financial system were performed within that system's test environment. However, CBP personnel were unable to provide evidence in a timely manner that the test environment was appropriately mirrored with the production environment.
- Configuration changes to financial systems were not consistently tested before deployment to production.

*IT Application Controls*

- 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.
- CBP was unable to identify an appropriate point of contact to demonstrate application control procedures for one financial process area.

**Recommendations**

We recommend that the CBP Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO) make the following improvements to CBP's financial management systems and associated IT security program (in accordance with CBP and DHS requirements, as applicable):

*Security Management*

- Improve and monitor existing security awareness and role-based training programs to ensure that training is completed in a timely manner and that financial system access is only granted after completion of training requirements.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

- Implement processes to monitor the status of agreements to ensure that ISAs are renewed and approved by required stakeholders timely.

*Access Controls*

- Conduct additional training with responsible personnel to ensure that existing procedures for authorizing and recertifying application access are performed consistently. Where appropriate, centralize application access administration functions within in one organization to reduce the number of control owners and the corresponding risk of inconsistent control execution.
- Develop and implement processes to document, review, approve, and maintain evidence of authorization for administrator or other highly-privileged access to financial system components, including controls to prevent violations of the principles of least privilege and segregation of duties in provisioning access.
- Implement, sustain, or enhance existing controls to conduct periodic reviews of all accounts on financial system components, including identification of inappropriately unlocked service accounts and violations of the principles of least privilege and segregation of duties, and removal of accounts deemed no longer necessary.
- Implement technical solutions and monitoring controls to improve the timeliness of communicating notifications of separating employees to system owners.
- Finalize and communicate guidance to Contracting Officers' Representatives and other accountable stakeholders, and implement monitoring controls to improve timeliness of communicating notifications of separating contractors to system owners.
- Implement technical solutions and monitoring controls to prevent developers from having production access to migrate code to application production environments and to periodically review, monitor, and retain logs of the activity of individuals granted permission to develop and migrate code to production.
- Establish and provision individual user accounts to ensure that developer actions can be individually attributed, monitored and tracked.
- Where segregation of duties violations existed relative to developer access to production during FY 2014, perform an analysis over implemented application functionality to identify any potential unauthorized or inappropriate modifications and their corresponding financial statement impact.
- Implement configurations to disable all system accounts after 45 days of inactivity.
- Implement processes and procedures to ensure that all events subject to audit logging on financial system components are reviewed on an annual basis, audit events are captured in a human-readable

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

format, all audit logs are periodically reviewed by security management personnel, and suspicious activity is appropriately escalated.

- Implement controls to prevent unauthorized modification, access, or destruction of audit log files.

*Configuration Management*

- Implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during the vulnerability assessment.
- Implement controls to conduct periodic vulnerability scans over all financial system components, review scan results, and, as required based on scan results, initiate appropriate remediation efforts.
- Continue planned efforts to migrate financial applications currently residing on unsupported system software so that appropriate vendor patches can be applied to address known vulnerabilities.
- Document and implement a strategy for validating that functionality within application production and test environments are identical.
- Conduct additional training with responsible personnel, and implement additional monitoring controls, to ensure that existing procedures for appropriately testing changes prior to implementation into the production environment are performed consistently.

*IT Application Controls*

- Implement processes to identify backup personnel prior to personnel transitions to ensure that functions related to financial process control areas can continue to be performed.
- Continue to pursue technical solutions and monitoring controls to reduce the risk of overpayment and revenue loss exposure over drawback claims.

## **OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY**

To complement our IT controls test work during the FY 2014 audit, we performed additional non-technical information security procedures at CBP. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where CBP personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These procedures were performed in accordance with the FY 2014 STAL, signed by DHS OIG management, KPMG management, and DHS management (Chief Information Officer [CIO], Chief Information Security Officer, Chief Financial Officer, Chief Privacy Officer, and Chief Security Officer) on June 3, 2014, and transmitted to the DHS CIO Council on June 12, 2014.

### **Social Engineering**

Social engineering is defined as the act of manipulating people into performing actions or divulging sensitive information. The term typically applies to trickery or deception for the purpose of information gathering or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which CBP personnel were willing to divulge network or system passwords that, if exploited, could compromise CBP sensitive information.

To conduct this testing, we made phone calls from various CBP locations at various times throughout the audit. Posing as CBP technical support personnel, we attempted to solicit access credentials from CBP users. Attempts to login to CBP systems were not performed; however, we assumed that disclosed passwords that met the minimum password standards established by DHS policy were valid exceptions. During social engineering performed at CBP, we attempted to call a total of 60 employees and contractors and reached 51. Of those 51 individuals with whom we spoke, one divulged their password in violation of DHS policy.

The selection of attempted or connected calls was not statistically derived, and, therefore, the results described here should not be used to extrapolate to CBP as a whole.

### **After-Hours Physical Security Walkthroughs**

Multiple DHS policies, including the DHS Sensitive Systems Policy Directive 4300A, the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally-Identifiable Information (PII)*, and DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive but Unclassified (FOUO) Information*, mandate the physical safeguarding of certain materials and assets which, if compromised either due to external or insider threat, could result in unauthorized access, disclosure, or exploitation of sensitive IT or financial information.

We performed procedures to determine whether CBP personnel consistently exercised responsibilities related to safeguarding sensitive materials as defined in these policies. Specifically, we performed escorted walkthroughs of workspaces – including cubicles, offices, shared workspaces, and/or common areas (e.g.: areas where printers were hosted) – at CBP facilities that processed, maintained, and/or had access to financial data during FY 2014. We inspected workspaces to identify instances where materials

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from CBP, DHS OIG and DHS OCIO.

During after-hours physical security walkthroughs performed at CBP, we inspected a total of 120 workspaces. Of those, 26 were observed to have material – including, but not limited to, system passwords, information marked “FOUO” or otherwise meeting the criteria established by DHS MD 11042.1, documents containing sensitive PII, and government-issued storage media – left unattended and unsecured after business hours in violation of DHS policy.

The selection of inspected areas was not statistically derived, and, therefore, the results described here should not be used to extrapolate to CBP as a whole.



## **Appendix A**

### **Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2014 CBP Consolidated Financial Statement Audit**

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

Below is a description of the significant CBP financial management systems and supporting IT infrastructure included in the scope of the FY 2014 CBP consolidated financial statement audit.

Automated Commercial Environment (ACE)

ACE is a web-based major application that is used by CBP 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. It includes functionality to calculate monthly statements for importers and perform sampling and audits of import/entry transactions. It was developed to replace the Automated Commercial System (ACS).

ACE collects duties at ports, collaborates with financial institutions to process duty and tax payments, and provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations, illegal imports and terrorist activities.

ACE contains interfaces with ACS, other internal CBP feeder systems, and external service providers (including the Department of Transportation's Federal Motor Carrier Safety Administration and the Office of Naval Intelligence Global Trader system).

ACE is developed and maintained by the CBP Cargo Systems Program Directorate (CSPD) and the Enterprise Data Management and Engineering Directorate (EDMED), and hosted and supported by the CBP Office of Information and Technology exclusively for internal use by the CBP user community. In addition to CBP, users of ACE include other participating government agency personnel and non-governmental (private) trade professionals.

Automated Commercial System (ACS)

ACS is a mainframe-based major application that is comprised of subsystems used by CBP 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. It includes functionality to calculate monthly statements for importers and perform sampling and audits of import/entry transactions.

ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, and provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations, illegal imports and terrorist activities.

ACS contains interfaces with internal CBP feeder systems and external service providers (including various affiliated financial institutions, the Food and Drug Administration's Mission Accomplishment Regulatory Compliance Services program, the Internal Revenue Service Web Currency and Banking Retrieval System, and the U.S. Department of Agriculture (USDA) Animal and Plant Health Inspection Service).

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

ACS was developed and is maintained by CBP CSPD and EDMED, and hosted and supported by the CBP Office of Information and Technology for internal use by the CBP user community. In addition to CBP, users of ACS include USDA, the Centers for Disease Control and Prevention, the United States Coast Guard, and non-governmental (private) trade professionals.

Systems, Applications, and Products (SAP)

SAP is a client/server-based major application and the official accounting system of record for CBP. It is an integrated financial management system used to manage assets (e.g., budget, logistics, procurement, and related policy) and revenue (e.g., accounting and commercial operations: trade, tariff, and law enforcement), and to provide information for strategic decision making. CBP's SAP instance includes several modules that provide system functionality for funds management, budget control, general ledger, real estate, property, internal orders, sales and distribution, special purpose ledger, and accounts payable activities, among others.

SAP contains interfaces with internal CBP feeder systems, including ACE and ACS, and external service providers (including the General Services Administration's Next Generation Federal Procurement Data System, U.S. Department of the Treasury Bureau of the Fiscal Service and FedTraveler.com E-Gov Travel Service).

SAP is developed and maintained by the CBP Border Enforcement & Management Systems Directorate program office and EDMED, and hosted and supported by the CBP Office of Information and Technology (OIT) exclusively for internal use by the CBP financial user community.

Computerized Aircraft Reporting and Material Control System (CARMAC)

CARMAC is a mainframe-based major application used by CBP to track and record aircraft maintenance inspections and related activities such as the inventory of spare parts, special tools, and support equipment, as well as corresponding financial support.

CARMAC is developed and maintained by the CBP Office of Air and Marine (OAM) and the CBP OIT and hosted and supported by CSC contractor personnel exclusively for internal use by the CBP OAM and Defense Support Services user community.

Active Directory (AD) / Authorized Desktop Build (ADB)

The CBP AD and ADB GSS provide IT desktop access, tools, and resources necessary for CBP employee and contractors to support the mission of CBP operational elements. This end-user computing environment includes connectivity to regional local area networks across the United States and manages the deployment and configuration of back-office and mission desktop software.

The AD and ADB GSS environment is maintained by CBP EDMED and hosted and supported by CBP OIT exclusively for internal use by the CBP user community.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Customs and Border Protection*  
September 30, 2014

---

## **Appendix B**

### **FY 2014 IT Notices of Findings and Recommendations at CBP**

Department of Homeland Security  
*Information Technology Management Letter*  
 U.S. Customs and Border Protection  
 September 30, 2014

| <b>FY 2014 NFR #</b> | <b>NFR Title</b>   | <b>FISCAM Control Area</b> | <b>New Issue</b> | <b>Repeat Issue</b> |
|----------------------|--|----------------------------|------------------|---------------------|
| CBP-IT-14-01         | Security Awareness Issues Identified during After-Hours Physical Security Testing at CBP   | Security Management        |                  | X                   |
| CBP-IT-14-02         | Security Awareness Issues Identified during Social Engineering Testing at CBP  | Security Management        | X                |                     |
| CBP-IT-14-03         | Separated Personnel on SAP Application User Listing  | Access Controls            |                  | X                   |
| CBP-IT-14-04         | Lack of Annual Recertification of SAP Oracle Database Accounts; Weaknesses in SAP Oracle Database (DB) Service Accounts Retaining Unnecessary Access | Access Controls            | X                |                     |
| CBP-IT-14-05         | Deficiencies in the Controls for Creating New ACS Application Accounts   | Access Controls            |                  | X                   |
| CBP-IT-14-06         | ACS Application Recertification Weaknesses   | Access Controls            |                  | X                   |
| CBP-IT-14-07         | Separation of Duties Weaknesses over the ACS Application and Mainframe Security Control Accessor Administrators                                      | Access Controls            | X                |                     |
| CBP-IT-14-08         | Lack of Review of ACE Linux Operating System (OS) Audit Logs & Annual Audit Log Parameters   | Access Controls            | X                |                     |
| CBP-IT-14-09         | Lack of Review of ACE Oracle DB Audit Logs & Annual Audit Log Parameters   | Access Controls            | X                |                     |
| CBP-IT-14-10         | Lack of Annual Recertification of ACE Linux OS Administrators  | Access Controls            | X                |                     |
| CBP-IT-14-11         | Lack of Annual Recertification of ACE Oracle DB Accounts and Deficiencies in ACE Oracle DB General Administrators Retaining Unnecessary Access       | Access Controls            | X                |                     |

Department of Homeland Security  
*Information Technology Management Letter*  
 U.S. Customs and Border Protection  
 September 30, 2014

| <b>FY 2014 NFR #</b> | <b>NFR Title</b>  | <b>FISCAM Control Area</b> | <b>New Issue</b> | <b>Repeat Issue</b> |
|----------------------|---|----------------------------|------------------|---------------------|
| CBP-IT-14-12         | Lack of ACE Linux OS Inactivity Parameters  | Access Controls            | X                |                     |
| CBP-IT-14-13         | Separated Personnel on the ACS Application User Listing   | Access Controls            | X                |                     |
| CBP-IT-14-14         | Configuration Management and Separation of Duties Weaknesses within the ACE   | Configuration Management   | X                |                     |
| CBP-IT-14-15         | Lack of Monthly Vulnerability Scans Performed over the ACE  | Configuration Management   | X                |                     |
| CBP-IT-14-16         | Lack of Review and Protection of CARMAC Application and Mainframe Audit Logs  | Access Controls            | X                |                     |
| CBP-IT-14-17         | Weaknesses in Creating New CARMAC Time Sharing Option Mainframe Accounts  | Access Controls            | X                |                     |
| CBP-IT-14-18         | Lack of Patching Performed over the CARMAC Mainframe  | Configuration Management   | X                |                     |
| CBP-IT-14-19         | Separated Personnel on the ADB AD Network User Listing  | Access Controls            |                  | X                   |
| CBP-IT-14-20         | Failure to Identify Knowledgeable Personnel for Discussion Regarding Accelerated Payment Privileges   | Business Process Controls  | X                |                     |
| CBP-IT-14-21         | Inappropriately Configured Audit Log Parameters for SAP UNIX OS   | Access Controls            | X                |                     |
| CBP-IT-14-22         | Lack of Annual Recertification of CARMAC Application and Mainframe Generic, Non-human accounts; Deficiencies in CARMAC Application and Mainframe Generic, Non-human Accounts Retaining Unnecessary Access | Access Controls            | X                |                     |
| CBP-IT-14-23         | Weakness in Testing ACS Configuration Management Changes Prior to Implementation into the Production Environment  | Configuration Management   | X                |                     |
| CBP-IT-14-24         | Separated Personnel on the CARMAC Application User Listing  | Access Controls            | X                |                     |

Department of Homeland Security  
*Information Technology Management Letter*  
 U.S. Customs and Border Protection  
 September 30, 2014

| <b>FY 2014 NFR #</b> | <b>NFR Title</b>  | <b>FISCAM Control Area</b>                             | <b>New Issue</b> | <b>Repeat Issue</b> |
|----------------------|---|--|------------------|---------------------|
| CBP-IT-14-25         | Lack of Comparable ACS Test and Production Environments                                   | Business Process Controls/<br>Configuration Management | X                |                     |
| CBP-IT-14-26         | Inappropriately Configured Inactivity Parameters for the CARMAC Application and Mainframe | Access Controls  | X                |                     |
| CBP-IT-14-27         | Lack of ACE Oracle DB Inactivity Parameters   | Access Controls  | X                |                     |
| CBP-IT-14-28         | ACE Configuration Baseline Weaknesses   | Configuration Management                               | X                |                     |
| CBP-IT-14-29         | Lack of Functionality in the ACS  | Business Process Controls                              |                  | X                   |
| CBP-IT-14-30         | Deficiencies in Renewal of ISAs   | Security Management                                    | X                |                     |
| CBP-IT-14-31         | Deficiencies in Security Awareness and Role-based Training Programs                       | Security Management/<br>Access Controls                | X                |                     |



# OFFICE OF INSPECTOR GENERAL

## Department of Homeland Security

---

Washington, DC 20528

### **Report Distribution**

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
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 Privacy Officer

#### **U.S. Customs Border Protection**

Commissioner  
Chief Financial Officer  
Chief Information Officer  
Audit Liaison

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

#### **Congress**

Congressional Oversight and Appropriations Committees



## ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: [www.oig.dhs.gov](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov). Follow us on Twitter at: @dhsoig.



## OIG HOTLINE

To report fraud, waste, or abuse, visit our website at [www.oig.dhs.gov](http://www.oig.dhs.gov) and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Hotline  
245 Murray Drive, SW  
Washington, DC 20528-0305