

Information Technology Management Letter for the FY 2016 U.S. Customs and Border Protection Financial Statement Audit





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the FY 2016 U.S. Customs and Border Protection Financial Statement Audit

May 15, 2017

Why We Did This Audit

Each year, our independent auditors identify component-level information technology (IT) control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details that were not included in the fiscal year 2016 DHS Agency Financial Report.

What We Recommend

We recommend that CBP, in coordination with the DHS Chief Information Officer and Acting 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

What We Found

We contracted with the independent public accounting firm KPMG, LLP to perform the audit of U.S. Customs and Border Protection's (CBP) consolidated financial statements for the year ended September 30, 2016. KPMG evaluated selected general information technology controls (GITC), IT entity-level controls, and business process application controls at CBP. KPMG determined that CBP had made improvements by designing and implementing certain account management, audit logging, and configuration management controls.

However, KPMG continued to identify financial system functionality and GITC deficiencies related to access controls and configuration management for CBP's core financial, feeder, General Support Systems environments. The deficiencies collectively limited CBP's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability.



OFFICE OF INSPECTOR GENERAL

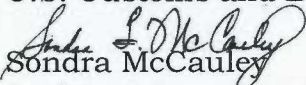
Department of Homeland Security

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

May 15, 2017

MEMORANDUM FOR: Phillip A. Landfried
Assistant Commissioner
U.S. Customs and Border Protection

Jaye M. Williams
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 2016 U.S. Customs and Border Protection Financial
Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2016 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 2016 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2016, which was included in the FY 2016 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2016 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 Kevin Burke, Acting Director, Information Systems and Acquisitions Division, at (202) 254-5450.

Attachment



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

January 18, 2017

Office of Inspector General
U.S. Department of Homeland Security
Washington, DC

Chief Information Officer and Chief Financial Officer
U.S. Customs and Border Protection
Washington, DC

Ladies and Gentlemen:

We planned and performed our audit of the consolidated financial statements of the U.S. Customs and Border Protection (CBP), as of, and for the year ended, September 30, 2016, in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*. We considered CBP's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of CBP's internal control. Accordingly, we do not express an opinion on the effectiveness of CBP's internal control.

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. 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 noted certain internal control deficiencies at CBP during our audit that, in the aggregate, represent a material weakness in general information technology (IT) controls and financial systems functionality at CBP, as reported in our *Independent Auditors' Report* dated January 18, 2017. Specifically, with respect to financial systems at CBP, we noted certain matters in the general IT control areas of access controls, configuration management, segregation of duties, and contingency planning, as well as in the area of business process application controls. These matters are described in the *Findings and Recommendations* section of this letter. Our findings over non-IT internal controls that did not aggregate to a significant deficiency or material weakness, as reported in the *Independent Auditors' Report*, are presented in a separate letter to the Department of Homeland Security (DHS) Office of Inspector General (OIG) and CBP Chief Financial Officer.

Additionally, at the request of the DHS OIG, we performed additional non-technical information security procedures to identify instances in which 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 subject to audit procedures in *Appendix A*, and a listing of each IT internal control deficiency identified during our audit of the consolidated financial statements as of, and for the year ended September 30, 2016 in *Appendix B*.

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

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, 2016

TABLE OF CONTENTS

	Page
Objective, Scope and Approach	2
Summary of Findings	4
Findings and Recommendations	5
Findings	5
Recommendations	7
Observations Related to Non-Technical Information Security	10

APPENDICES

Appendix	Subject	Page
Appendix A	Description of Key CBP Financial Systems and IT Infrastructure	12
Appendix B	FY 2016 IT Notices of Findings and Recommendations	17

OBJECTIVE, SCOPE, AND APPROACH

Objective

We audited the consolidated financial statements of CBP as of and for the year ended September 30, 2016. In connection with our audit of these consolidated financial statements, we performed an evaluation of CBP general information technology controls (GITC), IT entity-level controls (ELC), and IT application controls to assist in planning and performing our audit engagement. At the request of the DHS 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 U.S. Government Accountability Office (GAO) issued the *Federal Information System Controls Audit Manual* (FISCAM), which formed the basis for 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. It 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 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.

Although each of these FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs 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 that depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2016 GITC procedures at CBP did not necessarily represent controls from each FISCAM category.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

Business Process Application Controls

Where relevant GITCs were operating effectively, we tested selected IT application controls (process-level controls — fully automated or manual with an automated component) on financial systems and applications to assess internal controls over input, processing, and output of financial data and transactions.

FISCAM defines Business Process Application Controls (BPAC) as the automated and/or manual controls applied to business transaction flows; and related to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. BPACs 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 IT application controls 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 2016, 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 component 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 2016 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG LLP, DHS OIG, and DHS management.

Appendix A provides a description of the key CBP financial systems and IT infrastructure subject to audit procedures in the current fiscal year.

SUMMARY OF FINDINGS

During our FY 2016 assessment of GITCs and BPACs performed in connection with the financial statement audit, we determined that CBP made progress in remediating certain IT control deficiencies reported in FY 2015. For example, CBP made improvements by designing and implementing certain account management, audit logging, and configuration management controls. However, we continued to identify BPAC deficiencies related to financial system functionality, as well as GITC deficiencies related to access controls (including, but not limited to, the review of audit logs and the management of access to system components) and configuration management for CBP's core financial and feeder systems and associated General Support System (GSS) environments. In many cases, new control deficiencies reflected weaknesses over new systems or new controls in scope for FY 2016 that 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 as to ensure confidentiality, integrity, and availability. In addition, certain of these deficiencies at CBP adversely impacted the internal controls over CBP's financial reporting and their operation, and we consider them to collectively represent a material weakness for CBP under standards established by the American Institute of Certified Public Accountants and the U.S. GAO.

Of the 39 IT Notices of Findings and Recommendations (NFR) issued during our FY 2016 testing, 19 were repeat findings, either partially or in whole from the prior year, and 20 were new findings. The 39 IT NFRs represent deficiencies and observations related to all five FISCAM GITC categories, as well as in the area of BPACs.

The majority of the deficiencies that our audit identified were related to non-compliance with financial system controls. According to DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and CBP policies, financial system controls lacked proper documentation, were not fully designed, were inadequately detailed, and were inconsistently implemented. The most significant weaknesses from a financial statement audit perspective continued to include:

1. excessive, unauthorized, or inadequately monitored access to system components for key CBP financial applications;
2. audit logging controls that were not fully defined, followed, or effective;
3. a lack of proper segregation of duties for roles and responsibilities within financial systems and infrastructure layers; 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 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.

Although the recommendations we made should be considered by CBP, it is ultimately the responsibility of CBP management to determine the most appropriate methods for addressing the deficiencies identified.

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2016 CBP consolidated financial statements, we identified the following GITC deficiencies, certain of which, in the aggregate, contributed to the IT material weakness:

Access Controls

- Strong password, inactivity, and account and data protection requirements were not consistently enforced on operating systems supporting financial applications.
- Audit logs for multiple financial system components (including the application, database, and operating system/mainframe layers), were not reviewed on the prescribed basis, did not include all required auditable events at an adequate level of detail, were not reviewed annually to verify the continued appropriateness of relevant security events subject to logging, and were not adequately protected from unauthorized modification or deletion.
- Audit log review activities on multiple financial system components (including the application, database, and operating system/mainframe layers) were not consistently implemented. Deficiencies included failure to document the review, not maintaining evidence of the review, not following the documented process, not having a process documented to review activities performed by temporary users, and failure to use an independent party.
- Recertification of system user accounts (including the application, database, operating system, and network layers) was not designed and/or operating effectively. Deficiencies included not having a sufficiently detailed documented process, not maintaining evidence that a recertification was completed, not including all user roles, recertifying incorrect users and/or accounts, and users performing reviews of their own accounts.
- Account management activities were not consistently or timely documented or implemented. Deficiencies included not having a documented account authorization process, not maintaining access authorization documentation, providing access before the date the access was approved, and not having separate individuals approve and grant access.
- Policies and procedures for managing and authorizing elevated administrator-level access were not consistently or completely developed and formally documented.
- Recertification of developers and individuals who can migrate changes to production was not performed.
- Application users were not timely removed upon their separation from CBP.

Configuration Management

- Test plans, test results, and change authorizations prior to development and implementation of changes were not formally documented for one system.
- Controls to enforce segregation of duties between developers possessing the ability to modify application functionality and migrate changes to production were inadequate.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

- Monthly database vulnerability scans were not performed for the entire fiscal year in accordance with CBP policy.
- Certain configuration-related deficiencies identified on servers, workstations, and system software were not remediated within a timely manner and tracked appropriately for remediation within management's Plan of Actions and Milestones (POA&M).

Segregation of Duties

- Processes for enforcing segregation of duties and least privilege were inadequate. Deficiencies included, but were not limited to, not documenting procedure/policy for detailing segregation of duties and not identifying risks of certain administrative roles.
- Controls to enforce segregation of duties among users who had access to the database and operating systems were inadequate.

Contingency Planning

- Daily and weekly system backups were not successfully performed and retained for one financial system.

IT Application Controls

- One financial system lacked the controls necessary to prevent or detect and correct excessive drawback claims. Specifically, the programming logic for the system did 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.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

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):

Access Controls

- Implement technical controls to ensure that passwords for operating systems supporting financial systems are configured in accordance with DHS requirements, and monitor the password parameters to ensure they remain in compliance.
- Design and implement audit log processes that address the frequency for log reviews, frequency for configuration setting reviews, documentation that must be maintained from log reviews, correlation of activity in logs to individual user accounts, configuration of logs to capture adequate detail, separation of duties of users who can create/modify/delete logs, and procedures for granting temporary and/or ad hoc user access to logs.
- Design a process and perform risk assessments of the current audit log review process and document the results.
- Complete the implementation and configuration of an audit log tool to facilitate log reduction and monitoring, and separate storage of audit log results.
- Designate an independent party to review audit logs.
- Perform risk assessments of current recertification processes, create and/or update a formal annual recertification process, and provide training to those individuals who perform user recertification.
- Conduct recertification of system accounts in accordance with policy and maintain evidence of the results.
- Design and implement a process for ensuring a complete and accurate listing of all users to be recertified.
- Explore the possibility of implementing an automated mechanism for recertification of all users.
- Create and/or update current policies and procedures for account access authorization and management, provide training to personnel who are responsible for account management, and establish a central location for maintaining access authorization documentation.
- Perform a risk assessment of the process for providing system access to privileged users, and create and implement a formal process for reviewing and authorizing the privileged access.
- Create and implement a formal annual recertification process for developers and production migrators, and train individuals responsible for performing the recertification.
- Remove system access for separated users. This would include developing and implementing a process for removing separated employee access, providing training to personnel on the process, and exploring the

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

possibility of implementing an automated mechanism to remove user accounts when a separation is processed.

- Continue to effectively perform the implemented processes and controls over identified conditions that were effectively remediated during FY 2016.

Configuration Management

- Create a formal process for documenting and maintaining test plans and test results and provide training to individuals who perform the testing.
- Perform risk assessments on segregation of duties and least privilege principles for individuals with access to development and production code libraries, and create and implement a process to enforce segregation of duties for the development and production code libraries.
- Create a standard operating procedure for database vulnerability scanning, perform monthly database scans, and train personnel to ensure they are aware of vulnerability scanning requirements.
- Ensure vulnerability scans are performed consistently using DHS Secure Baseline Configuration Guides and make certain documentation of these scans are reviewed and maintained so that follow-up and remediation can be conducted.
- Continue to effectively perform the implemented processes and controls over identified conditions that were effectively remediated during FY 2016.

Segregation of Duties

- Perform risk assessments of segregation of duties and least privilege principles for users with administrative roles, and document risk acceptance for any conflicting roles that have valid business justification.
- Design, disseminate, and implement processes for performing segregation of duties reviews.
- Define and implement guidance for granting layers of access to ensure that proper segregation of duties and least privilege principles are followed.
- Continue to effectively perform the implemented processes and controls over identified conditions that were effectively remediated during FY 2016.

Contingency Planning

- Design, disseminate, and implement a process to perform successful system backups, maintain evidence of the backups, and train personnel on backup policies and procedures.
- Continue to effectively perform the implemented processes and controls over identified conditions that were effectively remediated during FY 2016.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

IT Application Controls

- Pursue technical solutions and monitoring controls to reduce the risk of overpayment and revenue loss related to drawback claims.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2016 audit, we performed additional non-technical information security procedures at CBP. These procedures included after-hours physical security walkthroughs to identify instances in which 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 2016 *Security Testing Authorization Letter* (STAL) signed by DHS OIG management, KPMG management, and DHS management.

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 gathering information or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which CBP component 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 log into 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 four. Of those four individuals with whom we spoke, none divulged passwords in violation of DHS policy.

The selection of attempted or connected calls was not statistically derived; 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 (SBU) (FOUO) Information*, mandate the physical safeguarding of certain materials and assets that, 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 2016. We inspected workspaces to identify instances where materials 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, 32 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 and laptops – left unattended and unsecured after business hours in violation of DHS policy.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

The selection of inspected areas was not statistically derived; 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

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

Below is a description of significant CBP financial management systems and supporting IT infrastructure included in the scope of the FY 2016 financial statement audit.

Automated Commercial Environment (ACE)

ACE is a web-based major application that CBP uses to track, control, and process commercial goods and conveyances entering the United States 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. ACE is being developed to replace the Automated Commercial System (ACS), with target completion by early calendar year 2017.

ACE 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, 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's Global Trade system).

The CBP Cargo Systems Program Directorate (CSPD) and the Enterprise Data Management and Engineering Directorate (EDMED) developed and maintain ACE. The CBP Office of Information and Technology (OIT) hosts and supports ACE for a user community comprising CBP personnel, participating government agency personnel, and non-governmental (private) trade professionals.

The application is hosted in Springfield, VA. Oracle Linux, Red Hat Enterprise Linux, and AIX operating system servers, as well as Oracle and IBM DB2 databases support it.

Automated Commercial System (ACS)

ACS is a mainframe-based major application comprising subsystems CBP uses to assess the duties, fees, and taxes owed to the Federal government on any commercial goods and conveyances being imported into the United States territory and to track any refunds on those duties. It includes functionality to calculate monthly statements for importers, and to perform sampling and audits of import/entry transactions. ACS is being decommissioned by functionality/module and replaced by ACE with target completion by early calendar year 2017.

ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, and provides automated duty filing for trade clients. The application also 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 (MARCS) program, the Internal Revenue Service's Web Currency and Banking Retrieval System, and the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service.

CBP's CSPD and EDMED developed and maintain the ACS application. CBP OIT hosts and supports the application for a user community comprising CBP, USDA, the Centers for Disease Control and Prevention, the United States Coast Guard, and non-governmental (private) trade professionals.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

The application is hosted in Springfield, VA, and the IBM z/OS mainframe, as well as Computer Associates (CA) Datcom and IBM DB2 databases support it.

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

SAP ECC is a client/server-based major application, with configurable web access, and the official accounting system of record/general ledger for CBP. It is an integrated financial management system used to account for assets (e.g., budget, logistics, procurement, and related policy) and revenue (e.g., accounting and commercial operations including 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. Data resulting from transactions that SAP ECC processes interfaces with SAP BW, which is optimized for query and report generation.

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

The CBP Border Enforcement and Management Systems Directorate (BEMSD) program office and EDMED developed and maintain SAP, and CBP OIT hosts and supports the application exclusively for the internal CBP financial user community.

The application is hosted in Springfield, VA, and Solaris Unix operating system servers and Oracle databases support it.

CBP Overtime Scheduling System (COSS)

COSS is a mainframe-based application that CBP uses to track personnel, schedule and assign data, maintain projected and actual costs, monitor staffing, manage budgets, and support entry and approval of timesheets. COSS has a related mobile implementation, hosted on a mainframe through the use of Oracle middleware.

COSS interfaces with SAP to transfer cost data, and with the Time and Attendance Management System (TAMS) to transfer payroll-specific data for processing and eventual transmission to the USDA National Finance Center.

CBP's BEMSD and OIT developed and maintain COSS. CBP OIT hosts and supports the application for the internal CBP user community.

The application is hosted in Springfield, VA, and the IBM z/OS mainframe and CA Datcom databases support it.

Time and Attendance Management System (TAMS)

TAMS is a mainframe-based application CBP uses to process and transmit COSS data to the USDA National Finance Center. Prior to the development of COSS to meet expanding mission needs, TAMS was the main time and attendance application CBP used. Migration of TAMS functionality to COSS is ongoing, with a tentative completion date of 2018.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

CBP's BEMSD and OIT maintain TAMS. CBP OIT hosts and supports the application for the internal CBP user community.

The application is hosted in Springfield, VA, and the IBM z/OS mainframe and CA Datacom databases support it.

Seized Asset and Case Tracking System (SEACATS)

SEACATS is a mainframe-based application that enables the computerized tracking of all assets seized during CBP enforcement operations from the point when the asset is physically seized to the point when the asset is liquidated or related fines and penalties have been satisfied. In addition to tracking inventory, SEACATS serves as a repository for all case notes produced through the administrative and judicial processes related to the prosecution of seized asset offenses and the disposition of the involved assets.

SEACATS contains interfaces with internal CBP feeder systems, including SAP, ACE, and ACS. Two external service providers have access to SEACATS — the Department of Justice's (DOJ) Asset Management Forfeiture Staff and the U.S. Department of the Treasury (e.g., Treasury Executive Office for Asset Forfeiture, etc.).

SEACATS is currently undergoing development to modernize the application by 2018, although the production application is still legacy. CBP has also implemented a web-based SEACATS module to display Seizure Forms.

CBP BEMSD developed and maintains SEACATS. CBP OIT hosts and supports the application for the internal CBP user community, DOJ, and Treasury.

The application is hosted in Springfield, VA, and the IBM z/OS mainframe and CA Datacom databases support it.

Real Time Online Source Code Editor (ROSCOE)

ROSCOE is a mainframe-based subsystem used to edit, maintain, and submit job command language (JCL). Using JCL, direction can be written for the execution of basic mainframe-supported data processing. In this way, CBP uses ROSCOE to process, aggregate, or transform data for financial reporting purposes. Although ROSCOE may reference data held in other locations on the mainframe, it does not itself interface with any other subsystems or external applications.

EDMED hosts, supports, and maintains ROSCOE exclusively for the internal CBP user community.

CA Top Secret Security (TSS) Managed Mainframe Environment

The CA TSS package is the centralized security application that manages access to all Mainframe resources: the operating environments, databases, and initial access to resident applications such as ACS, COSS, TAMS, SEACATS, and ROSCOE. This end-user computing environment that CA TSS manages is a critical IT asset that supports all CBP employees and contractors in accomplishing the mission of CBP operational elements.

The Mainframe contains internal interfaces among hosted applications such as ACS, COSS, TAMS, and TECS. The Mainframe also connects with DHS OneNet, ACE, and SAP.

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
September 30, 2016

CBP's CSPD and EDMED developed and maintain CA TSS as well as general support services for the mainframe environment. CBP OIT hosts and supports the mainframe-supported applications for the internal CBP user community, as well as external trade users who transmit data to the applications.

Human Resource Business Engine (HRBE)

HRBE is a web-based, business process workflow management application implemented at CBP to simplify and automate human resources business processes across systems, organizations, and people. HRBE has been designed to automate workflow for hiring and pre-employment processing, labor relations, performance management, change management, and employee position management.

HRBE consumes data extracts from pre-employment testing vendors, Office of Personnel Management (OPM) job applicant data, and USDA National Finance Center bi-weekly payroll data.

HRBE contains interfaces with internal CBP feeder systems and operates strictly within DHS OneNet. CBP, U.S. Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), and DHS Headquarters employees and contract staff all use HRBE for different or all aspects of the aforementioned automated workflow functions.

CBP's Office of Human Resource Management (OHRM) developed and maintains HRBE. CBP OIT hosts and supports the application for the internal DHS user community.

The application is hosted in Springfield, VA, and the Microsoft Windows operating system servers and Microsoft SQL Server databases support it.

CBP Directory Services (CDS) / Authorized Desktop Build (ADB)

The CDS and ADB General Support Systems environment provides IT desktop access, tools, and resources necessary for CBP employees and contractors to support the mission of CBP operational elements in the National Capital Region (NCR). This end-user computing environment includes connectivity to regional local area networks (LANs) across the United States and manages the deployment and configuration of back-office and mission desktop software. CDS allows CBP to centralize access authentication and machine configuration management across all network resources, Microsoft servers, and databases using Organizational Unit and Group Membership.

CBP EDMED maintains the CDS and ADB General Support Systems environment, and CBP OIT hosts and supports the application exclusively for the internal CBP user community. The application is hosted in Springfield, VA, and Windows operating system servers support it.

Appendix B

FY 2016 IT Notices of Findings and Recommendations

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at CBP	Security Management		X
CBP-IT-16-02	Lack of CBP Overtime Scheduling System (COSS), Time and Attendance Management System (TAMS), and Seized Asset and Case Tracking System (SEACATS) Application Account Provisioning and Recertification Processes	Access Controls	X	
CBP-IT-16-03	Lack of Monitoring and Review of CBP Overtime Scheduling System (COSS), Time and Attendance Management System (TAMS), and Seized Assets and Case Tracking System (SEACATS) Application Audit Logs and Annual Audit Log Security Configurations	Access Controls	X	
CBP-IT-16-04	Ineffective Design of the Systems, Applications and Products (SAP) Database (DB) Audit Logging Process	Access Controls	X	
CBP-IT-16-05	Ineffective Design and Implementation of the Configuration and Review of Human Resources Business Engine (HRBE) Database (DB) Audit Logging	Access Controls		X
CBP-IT-16-06	Ineffective Design of the Systems, Applications and Products (SAP) Access and Separation of Duties Controls	Access Controls and Segregation of Duties	X	
CBP-IT-16-07	Ineffective Design of the Systems, Applications and Products (SAP) Application Audit Logging Process	Access Controls and Segregation of Duties	X	
CBP-IT-16-08	Ineffective Design of the Systems, Applications and Products (SAP) Oracle Database (DB) Audit Log Access Restriction Process	Access Controls		X
CBP-IT-16-09	Ineffective Design and Implementation of United States Department of Agriculture (USDA) Account Recertification Process	Access Controls	X	
CBP-IT-16-10	Lack of Annual Recertification of Automated Commercial Environment (ACE) Operating System (OS) and Database (DB) Accounts	Access Controls		X

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-11	Lack of Monthly Database Vulnerability Scanning Process	Configuration Management	X	
CBP-IT-16-12	Ineffective Design of Automated Commercial Environment (ACE) Change Management Separation of Duties	Access Controls, Segregation of Duties, and Configuration Management	X	
CBP-IT-16-13	Ineffective Controls over the Mainframe Application Change Management (CM) Separation of Duties and Account Recertification Processes	Access Controls and Configuration Management	X	
CBP-IT-16-14	Ineffective Controls Over Fiscal Year (FY) 2015 IT NFR Conditions During FY 2016	Access Controls, Segregation of Duties, Configuration Management, and Contingency Planning		X
CBP-IT-16-15	Lack of Monitoring and Review of Automated Commercial Environment (ACE) Oracle Database and Database Operating System Environment Audit Logs	Access Controls	X	
CBP-IT-16-16	Lack of Access Request and Authorization Process for Automated Commercial Environment (ACE) Database Operating System Administrators	Access Controls	X	
CBP-IT-16-17	Ineffective Controls over the Automated Commercial System (ACS) Application User Separation Process	Access Controls		X
CBP-IT-16-18	Ineffective Controls over the United States Department of Agriculture (USDA) User Account Creation Process	Access Controls	X	
CBP-IT-16-19	Ineffective Design of the Review and Protection of Human Resources Business Engine (HRBE) Operating System (OS) and CBP Directory Services (CDS) Audit Logs	Access Controls		X

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-20	Lack of Systems, Applications and Products (SAP) Application Developer Account Recertification Process	Access Controls and Configuration Management	X	
CBP-IT-16-21	Ineffective Design of Automated Commercial Environment (ACE) Exadata Database Operating System Environment Patching Process	Configuration Management	X	
CBP-IT-16-22	Lack of Review of Automated Commercial Environment (ACE) Database DB2 Audit Logs and Annual Audit Log Parameters	Access Controls	X	
CBP-IT-16-23	Ineffective Design of the Human Resources Business Engine (HRBE) Application Annual Audit Log Security Configuration Review	Access Controls		X
CBP-IT-16-24	Ineffective Controls over the Automated Commercial System (ACS) User Recertification Process	Access Controls		X
CBP-IT-16-25	Lack of Access Review over Automated Commercial Environment (ACE) Users	Access Controls	X	
CBP-IT-16-26	Ineffective Design of Human Resources Business Engine (HRBE) Separation of Duties Process	Access Controls and Segregation of Duties		X
CBP-IT-16-27	Ineffective Controls over the Human Resources Business Engine (HRBE) Account Management Process	Access Controls		X
CBP-IT-16-28	Ineffective Controls over Systems, Applications and Products (SAP) Change Management (CM) Separation of Duties	Configuration Management	X	
CBP-IT-16-29	Lack of Automated Commercial Environment (ACE) Application Developer and Production Migrator Account Recertification Process	Access Controls and Configuration Management	X	
CBP-IT-16-30	Ineffective Controls over the Human Resources Business Engine (HRBE) Application User Separation Process	Access Controls		X

Department of Homeland Security
Information Technology Management Letter
U.S. Customs and Border Protection
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-31	Ineffective Design of the Automated Commercial Environment (ACE) Red Hat Enterprise Linux (RHEL) Operating System and Oracle Database Environment Audit Logging Monitoring and Review Process	Access Controls	X	
CBP-IT-16-32	Ineffective Design of the Annual Recertification of Systems, Applications and Products (SAP) UNIX Operating System (OS) Accounts	Access Controls		X
CBP-IT-16-33	Ineffective Design of the CBP Cloud Computing Environment (C3E) and CBP Directory Services (CDS) Account Recertification Processes	Access Controls		X
CBP-IT-16-34	Ineffective Controls over Systems, Applications, Products (SAP) UNIX Operating System (OS) Identification and Authentication Processes	Access Controls		X
CBP-IT-16-35	Weaknesses Identified during the Vulnerability Assessment of the Authorized Desktop Build (ADB), CBP Directory Services (CDS), Human Resource Business Engine (HRBE), and Systems, Applications and Products (SAP) Environment	Configuration Management		X
CBP-IT-16-36	Ineffective Controls over the Automated Commercial System (ACS) User Account Creation Process	Access Controls		X
CBP-IT-16-37	(Withdrawn)	N/A	N/A	N/A
CBP-IT-16-38	Ineffective Controls over the Systems, Applications and Products (SAP) Application Access Separation Process	Access Controls		X
CBP-IT-16-39	Ineffective Controls over the Human Resources Business Engine (HRBE) Weekly Backups	Contingency Planning	X	
CBP-IT-16-40	Lack of Functionality in the Automated Commercial System (ACS)	Business Process Application Controls		X



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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 and 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.

For further information or questions, please contact Office of Inspector General Public Affairs at: 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 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