OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the FY 2015 U.S. Customs and Border Protection Financial Statement Audit

Homeland Security

May 11, 2016

OIG-16-68

DHS OIG Highlights

Information Technology Management Letter for the FY 2015 U.S. Customs and Border Protection Financial Statement Audit

May 11, 2016

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 (FY) 2015 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

What We Found

We contracted with the independent public accounting firm KPMG, LLP to perform the audit of the consolidated financial statements of the U.S. Customs and Border Protection (CBP) for the year ended September 30, 2015. KPMG evaluated selected general IT controls, entity level controls, and business process application controls at CBP. KPMG determined that CBP made improvements in designing and consistently implementing certain account management controls, audit logs, and interconnection security agreements.

However, KPMG continued to identify financial system functionality and GITC deficiencies related to logical access and configuration management for CBP's core financial and feeder systems. 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 their confidentiality, integrity, and availability.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 11, 2016

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

Jaye M. Williams
Chief Financial Officer
U.S. Customs and Border Protection

Sondra L McCauley

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

SUBJECT: *Information Technology Management Letter for the FY 2015 U.S. Customs and Border Protection Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2015 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 2015 Financial Statements and Internal Control over Financial Reporting*, dated November 13, 2015, which was included in the FY 2015 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2015 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 Huiswood, Director, Information Systems and Acquisitions Division, at (202) 254-5451.

Attachment

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

December 20, 2015

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, 2015, (hereinafter, referred to as the "fiscal year (FY) 2015 CBP consolidated financial statements"), 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 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. 15-02. 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 material weakness 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 - 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, 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.

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 2015 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. We communicated these matters 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 2015 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

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	4
Findings and Recommendations	6
Findings	6
Recommendations	8
Observations Related to Non-Technical Information Security	11

APPENDICES

Appendix	**Subject**	**Page**
A	Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2015 CBP Consolidated Financial Statement Audit	13
B	FY 2015 IT Notices of Findings and Recommendations at CBP	19

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, 2015, (hereinafter, referred to as the "fiscal year (FY) 2015 CBP consolidated financial statements"). In connection with our audit of the FY 2015 CBP consolidated financial statements, we performed an evaluation of selected CBP general information technology (IT) controls (GITCs), IT entity-level controls (ELCs), and IT application controls 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 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. 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 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.

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 that depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2015 GITC and IT ELC procedures at each DHS component 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 IT application controls (process-level controls that 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 Business Process Application Controls (BPACs) 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. 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 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 2015, 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 2015 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 within the scope of the FY 2015 DHS financial statement audit.

SUMMARY OF FINDINGS

During FY 2015, we noted that CBP took corrective action to address certain prior year IT control deficiencies. For example, CBP made improvements by designing and implementing certain account management, audit logging, and Interconnection Security Agreement controls. However, we continued to identify BPAC deficiencies related to financial system functionality, and 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 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 2015 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 and DHS' financial reporting and their operation, and we consider them to collectively represent a material weakness 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 28 IT Notices of Findings and Recommendations (NFRs) issued during our FY 2015 testing, five were repeat findings, either partially or in whole from the prior year, and 23 were new findings. The 28 IT NFRs issued represent deficiencies and observations related to all 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. Non-compliant configuration of system parameters;
3. Configuration management controls that were not fully defined, followed, or effective;
4. Lack of proper segregation of duties for roles and responsibilities within financial systems and infrastructure layers; and
5. 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. As noted in the DHS *Independent Auditors' Report*, 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 2015 CBP consolidated financial statements, we identified the following GITC and IT ELC deficiencies, certain of which, in the aggregate, contribute to the IT material weakness 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 were not consistently completed prior to granting system or network access or within required timeframes.

- One authority to operate (ATO) letter was expired and not renewed in a timely manner.

Access Controls

- Account security controls for multiple financial system components (including the application, database, and mainframe layers) were not fully designed and implemented, including password parameters.

- Audit logs for multiple financial system components (including the application, database, and operating system/mainframe layers) did not restrict system administrator access privileges over the audit logs, were not reviewed monthly as required, 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.

- Recertification of system accounts (including the application, database, operating system, and network layers) was not performed, did not include a complete and accurate listing of all user accounts, and lacked a sufficiently detailed recertification policy.

- Account management activities on multiple financial system components (including the application, database, and operating system/mainframe, and network layers) were not consistently or timely documented or implemented. Deficiencies included not revoking access from separated or transferred Federal employees and contractors, not maintaining access authorization documentation, providing access before the date the access was approved, providing roles that were not authorized, and not disabling or deleting inactive accounts.

- Account management activities for elevated access, including administrator-level access on multiple financial systems components (such as application, database, and operating system layers), were not consistently implemented. Deficiencies included providing access without authorization documentation, providing roles that were not authorized, and not suspending accounts that had passwords older than ninety (90) days.

- Generic service account logins were not acted upon when reviewed for abnormal activity.

- Account management activities for the mainframe system, non-human accounts (e.g., accounts that perform automated tasks and nightly batch jobs) were not consistently implemented. Deficiencies included not annually recertifying accounts as required, configuring accounts without establishing parameters for password expiration, providing accounts with certain access that allowed individuals to log into the mainframe environment without business justification, and establishing accounts with at least one administrative-level profile that allowed elevated access to the mainframe environment.

Configuration Management

- A process to configure financial application data protection settings had not been implemented.

- A process for maintaining application change documentation, including development authorization, test plans, authorization prior to implementation, and documentation indicating that separate users developed and deployed the change to production was not provided.

- Controls to enforce segregation of duties between developers having the ability to modify application functionality and migrate changes to production were inadequate.

- A process to comply with Information System Vulnerability Bulletin requirements or document waivers for non-compliant configurations was not implemented.

Segregation of Duties

- Controls to enforce segregation of duties among users who had access to the application, database, and operating systems were inadequate.

- Application permissions were granted in conflict with the principles of least privilege and separation of duties, and the extent of the separation of duties permission analysis and review was not sufficient.

Contingency Planning

- A process had not been designed and implemented to perform daily system backups for the virtual application servers for the entire fiscal year 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.

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.

- Enforce the DHS and CBP policies and procedures to ensure that ATOs are current.

Access Controls

- Conduct regular reviews to verify that identification and authentication parameters are configured in accordance with DHS and CBP policy.

- Conduct regular reviews of audit logs and parameters to identify any potential abnormal activity and verify that parameters are configured in accordance with DHS and CBP policy.

- Implement an enterprise-wide audit log solution/policy that includes detail on audit reduction and correlation tools, proper separation of duties of audit logs, and reviews are performed regularly by an independent party and documentation is maintained.

- Conduct recertification of system accounts in accordance with policy and maintain evidence of the recertification.

- Revise and implement the control policy to include a system-generated list of user accounts for access reviews.

- Implement configurations to disable all system accounts after 45 days of inactivity and update System Security Plans and policies and procedures to ensure compliance with DHS and CBP requirements.

- Implement and enforce account controls to ensure user access is removed or disabled when a user has separated or transferred.

- Update current account process documentation to promote the importance of retaining access authorization documentation, and modify training requirements to ensure that responsible personnel are aware of the current account provisioning and documentation retention procedures.

- Implement and disseminate account authorization management policies, require authorization prior to account provisioning, and only provision access/roles that were authorized.

- Refine and correct the process in place for disabling and deleting inactive user accounts and perform periodic reviews of inactivity controls.

- Revise, standardize, and implement a user access authorization policy to provide guidance for provisioning user accounts, recertifying accounts, and retaining documentation.

- Change all generic service accounts to system accounts.

- Remove unnecessary roles from system accounts to verify excessive access is not granted.

- Annually review all system, non-human accounts to ensure all accounts, including administrative profiles, have business justification and are compliant with relevant policy.

- Conduct an analysis of legacy system accounts and update access as necessary.

- Implement a process to configure the password expiration parameter settings on all system, non-human accounts, and/or document those system accounts that are exempt from the password expiration process to retain evidence of justification, authorization, and any necessary compensating controls.

- Update and/or implement additional processes to configure the Mainframe password settings, and document Mainframe departments whose accounts are exempted from the inactivity process in the Security Plan to retain evidence of justification, authorization, and any necessary compensating controls.

Configuration Management

- Update production client parameter settings in accordance with DHS and CBP policy, and conduct regular reviews to verify that production client settings are configured in accordance with DHS and CBP policy.

- Enhance, implement, and enforce configuration management policy to provide guidance for requiring authorization prior to implementation of a change, creating test plans, separating developer activities throughout the change process, and maintaining evidence the entire configuration management lifecycle.

- Improve and implement vulnerability management processes to ensure that any Common Vulnerability Exposures (CVEs) over 30 days are documented and remediated in a timely manner, including periodic reviews of the CVEs to verify that they are monitored and remediated in accordance with DHS and CBP policy.

Segregation of Duties

- Define and implement guidance for granting different layers of access to ensure proper segregation of duties and least privilege principles are followed.

- Perform and document regular reviews of access permissions to verify that segregation of duties across access layers is enforced and associated risks are mitigated.

Contingency Planning

- Formalize and document policy to enforce the performance of weekly backups of application servers, and obtain a waiver to exclude the performance of daily incremental/differential backups, as required by the CBP Handbook 1400-05D.

IT Application Controls

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

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2015 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 2015 STAL signed by DHS OIG management, KPMG management, and DHS management on May 20, 2015, and transmitted to the DHS CIO Council on May 27, 2015.

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 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 14. Of those 14 individuals with whom we spoke, two divulged passwords 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 (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 2015. 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, 34 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.

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 2015 CBP Consolidated Financial Statement Audit

Below is a description of the significant CBP financial management systems and supporting IT infrastructure included in the scope of the FY 2015 CBP consolidated 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 the end of calendar year 2016.

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).

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 (OIT) exclusively for internal use by the CBP user community. In addition to CBP, ACE users include other participating government agency personnel and non-governmental (private) trade professionals.

The application is hosted in Springfield, VA and is supported by Linux servers and Oracle and IBM DB2 databases.

Automated Commercial System (ACS)

ACS is a mainframe-based major application comprised of 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 track any refunds on those duties. It includes functionality to calculate monthly statements for importers and perform sampling and audits of import/entry transactions. ACS is being decommissioned by functionality/module and replaced by ACE with target completion by the end of calendar year 2016.

ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, and provides automated duty filing for trade clients. ACS 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.

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

The application is hosted in Springfield, VA and is supported by the IBM z/OS mainframe and IBM DB2 databases.

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

SAP ECC is a client/server-based major application and the official accounting system of record/general ledger 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. Data resulting from transactions processed by SAP ECC is interfaced to the SAP BW, which is optimized for query and report generation.

SAP contains interfaces with internal CBP feeder systems, including ACE and 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).

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

The application is hosted in Springfield, VA and is supported by Unix servers and Oracle databases.

CBP Overtime Scheduling System (COSS)

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

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

COSS is developed and maintained by CBP BEMSD and CBP OIT. The application is hosted and supported by CBP OIT for internal use by the CBP user community.

The application is hosted in Springfield, VA and is supported by the IBM z/OS mainframe and Computer Associates (CA) Datacom databases.

<u>Time and Attendance Management System (TAMS)</u>

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

TAMS is maintained by CBP BEMSD and CBP OIT. The application is hosted and supported by CBP OIT for internal use by the CBP user community.

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

<u>Seized Asset and Case Tracking System (SEACATS)</u>

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 related 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. SEACATS is accessed by two main external service providers, the Department of Justice's (DOJ) Asset Management Forfeiture Staff and the U.S. Department of the Treasury (Treasure 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.

SEACATS is developed and maintained by CBP BEMSD. The application is hosted and supported by CBP OIT for internal use by the CBP user community, DOJ, and Treasury.

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

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, ROSCOE is used by CBP to process, aggregate, or transform data for financial reporting purposes. While ROSCOE may reference data held in other locations on the Mainframe, it does not itself interface with any other subsystems or external applications.

ROSCOE is hosted supported and maintained by EDMED, exclusively for internal use by the CBP user community.

Computer Associates (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 managed by CA TSS is a critical IT asset that includes all CBP employees and contractors to support the mission of CBP operational elements.

The Mainframe contains internal interfaces among hosted applications such as ACS, COSS, TAMS, and the Traveler Enforcement Compliance System (TECS). The Mainframe also connects with DHS OneNet, ACE, and SAP.

Mainframe environment general support services and CA TSS are developed and maintained by CBP CSPD and EDMED, and hosted and supported by CBP OIT for internal use by the CBP user community, as well as external trade users that transmit data to Mainframe-supported applications.

Human Resource Business Engine (HRBE)

HRBE is a web-based application, business process workflow management tool 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 the 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 the HRBE application for different or all aspects of the aforementioned automated workflow functions.

HRBE is developed and maintained by the CBP Office of Human Resource Management (OHRM). The application is hosted and supported by CBP OIT for internal use by the DHS user community.

The application is hosted in Springfield, VA and is supported by Windows servers and SQL Server databases.

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) of the organization. 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.

The CDS and ADB General Support Systems environment is maintained by CBP EDMED, and hosted and supported by CBP OIT exclusively for internal use by the CBP user community.

The application is hosted in Springfield, VA and is supported by Windows servers.

Appendix B

FY 2015 IT Notices of Findings and Recommendations at CBP

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-15-01	Weaknesses in Systems, Applications, Products (SAP) UNIX Operating System (OS) Identification and Authentication Processes	Access Controls	X	
CBP-IT-15-02	Weaknesses in Systems, Applications, Products (SAP) UNIX Operating System (OS) and Oracle Database (DB) Audit Logging Processes	Access Controls	X	
CBP-IT-15-03	Lack of Annual Recertification of Systems, Applications, Products (SAP) UNIX Operating System (OS) System Accounts	Access Controls	X	
CBP-IT-15-04	Lack of Systems, Applications, Products (SAP) Inactive User Accounts Disablement	Access Controls	X	
CBP-IT-15-05	Weaknesses in Systems, Applications, Products (SAP) and Business Warehouse (BW) Client Configurations	Configuration Management	X	
CBP-IT-15-06	Weaknesses in Systems, Applications, Products (SAP) and Business Warehouse (BW) Access and Separation of Duties Controls	Access Controls	X	
CBP-IT-15-07	Weaknesses Related to Mainframe & TSS (Top Secret Security) Account Management	Access Controls	X	
CBP-IT-15-08	Weaknesses Related to Mainframe & TSS (Top Secret Security) Inactivity Management	Access Controls	X	
CBP-IT-15-09	Weaknesses Related to Mainframe & TSS (Top Secret Security) Audit Logging	Access Controls	X	
CBP-IT-15-10	Security Awareness Issues Identified during After-Hours Physical Security Testing at Customs and Border Protection (CBP)	Security Management		X
CBP-IT-15-11	Security Awareness Issues Identified during Social Engineering Testing at Customs and Border Protection (CBP)	Security Management		X

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-15-12	Weakness in Authorization to Operate Validity	Entity Level	X	
CBP-IT-15-13	Lack of Review and Protection of Human Resources Business Engine (HRBE) Database and Operating System Audit Logs	Access Controls	X	
CBP-IT-15-14	Weaknesses in the Human Resource Business Engine (HRBE) and CBP Directory Services (CDS) User Separation Process	Access Controls		X
CBP-IT-15-15	Weaknesses in the Review and Protection of Human Resources Business Engine (HRBE) Application and Audit Log Processes	Access Controls	X	
CBP-IT-15-16	Weakness in to CBP Directory Services (CDS) Account Provisioning Process	Access Controls	X	
CBP-IT-15-17	Weaknesses in the CBP Cloud Computing Environment (C3E) Account Recertification Process	Access Controls	X	
CBP-IT-15-18	Lack of Human Resources Business Engine (HRBE) Application Inactivity Guidance and Parameters	Access Controls	X	
CBP-IT-15-19	Lack of Human Resources Business Engine (HRBE) Operating System (OS) Daily Backups	Contingency Planning	X	
CBP-IT-15-20	Weaknesses in Human Resources Business Engine (HRBE) SQL (Structured Query Language) Serve Database Parameters	Access Controls	X	
CBP-IT-15-21	Weaknesses within Human Resources Business Engine (HRBE) Configuration Management and System Library Access Processes	Configuration Management	X	
CBP-IT-15-22	Weakness in Human Resources Business Engine (HRBE) Database (DB) Access Provisioning Process	Access Controls	X	

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-15-23	Weakness in CBP Directory Services (CDS) Inactive User Disablement Process	Access Controls	X	
CBP-IT-15-24	Weaknesses in the Human Resource Business Engine (HRBE) Account Management Process	Access Controls	X	
CBP-IT-15-25	Weaknesses in Human Resource Business Engine (HRBE) Separation of Duties Process	Access Controls	X	
CBP-IT-15-26	Weaknesses Identified during the Vulnerability Assessment of Human Resource Business Engine (HRBE) and Authorized Desktop Build (ADB)	Configuration Management	X	
CBP-IT-15-27	Deficiencies in Security Awareness and Role-based Training Programs	Security Management		X
CBP-IT-15-28	Lack of Functionality in the Automated Commercial System (ACS)	Entity Level		X

Appendix E
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.

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