OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the FY 2015 Department of Homeland Security Financial Statement Audit

Homeland Security

March 8, 2016
OIG-16-45

DHS OIG HIGHLIGHTS

Information Technology Management Letter for the FY 2015 Department of Homeland Security Financial Statement Audit

March 8, 2016

Why We Did This

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 the Chief Information Officer and Chief Financial Officer work with components to make improvements to DHS' financial management systems and associated IT 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. Department of Homeland Security (DHS) for the year ended September 30, 2015. KPMG LLP evaluated selected general IT controls, IT entity-level controls, and business process application controls at DHS components. KPMG determined that the DHS components had made progress in remediating certain IT deficiencies we reported in FY 2014. Approximately 48 percent of the prior year IT deficiencies identified were repeated.

The majority of the deficiencies identified by KPMG resulted from a lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program,* and National Institute of Standards and Technology guidance.

The deficiencies collectively limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability. The deficiencies at Customs and Border Protection, the United States Coast Guard, the Federal Emergency Management Agency, and U.S. Immigration and Customs Enforcement adversely impacted the internal controls over DHS' financial reporting and its operation, and collectively represent a material weakness reported in the FY 2015 DHS Agency Financial Report.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

March 8, 2016

MEMORANDUM FOR: Luke McCormack
Chief Information Officer

The Honorable Chip Fulghum
Deputy Under Secretary for Management
Chief Financial Officer

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

SUBJECT: *Information Technology Management Letter for the FY 2015 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2015 Department of Homeland Security 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 Huiswoud, Director, Information Systems Division, at (202) 254-5451.

Attachment

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

December 20, 2015

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

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department), as of and for the year ended September 30, 2015, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in 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 internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the consolidated financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

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

With respect to DHS and DHS Components' financial systems, we noted certain matters in the general IT control areas of security management, access controls, configuration management, segregation of duties, and contingency planning. We also noted certain matters related to limitations or weaknesses in system functionality that impacted the ongoing effective operation of general or process-level IT controls or contributed to other financial control deficiencies. These matters are described in the *Findings and Recommendations* section of this letter.

Additionally, at the request of the DHS OIG, we performed certain procedures to assess the adequacy of non-technical measures to secure sensitive IT and financial information and assets from unauthorized access or disclosure. We noted instances where DHS Component personnel

did not consistently apply the principles communicated in ongoing security awareness training related to these measures. These matters are described in the *Observations Related to Non-Technical Information Security Awareness Weaknesses* section of this letter.

We have provided a description of key DHS and Component financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit in Appendix A, and a listing of each IT Notice of Finding and Recommendation communicated to management during our audit in Appendix B.

Our audit procedures are designed primarily to enable us to form opinions on the financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of DHS'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.

DHS's response to the deficiencies identified in our audit is described in page 12 of this letter. DHS's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Very truly yours,

KPMG LLP

Department of Homeland Security
Consolidated Information Technology Management Letter
September 30, 2015

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

Objective

We audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2015 (referred to herein as the "fiscal year (FY) 2014 financial statements"). In connection with our audit of the FY 2015 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs), IT entity-level controls (ELCs), and IT application controls at DHS components 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 to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.
4. *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
5. *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

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 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 DHS components' 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. At many components, 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 DHS component 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 DHS and component financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2015 assessment of GITCs, IT ELCs, and IT application controls, we noted that the DHS components made progress in the remediation of certain IT findings we reported in FY 2014. We closed several of our prior year IT findings. However, new findings were noted in most DHS components in FY 2015, many of which were either (1) related to controls that were effective in prior years, or (2) control deficiencies noted over new systems that were similar to deficiencies previously reported.

In FY 2015, we issued 86 total findings, of which approximately 48 percent were repeated from the prior year. The new findings in FY 2015, noted at nearly all DHS components, resulted from additional IT systems and business processes within the scope of our audit this year and from control deficiencies identified in areas that were effective in previous years.

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

1. Excessive, unauthorized, or inadequately monitored access to, and activity within, key DHS financial applications, resources, and facilities;
2. Configuration management controls that were not fully defined, followed, or effective; and
3. Lack of proper segregation of duties for roles and responsibilities within financial systems.

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we noted that limitations in DHS components' financial systems' functionality may be inhibiting the Department's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data. At many components, key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Many key DHS 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*.

The conditions supporting our findings collectively limited DHS'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 Customs and Border Protection (CBP), the United States Coast Guard (Coast Guard), the Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE) adversely impacted the internal controls over DHS's financial reporting and its operation and we consider them to collectively represent a material weakness for DHS under standards established by the American Institute of Certified Public Accountants and the U.S. Government Accountability Office. Certain of the IT findings issued at CBP, Coast Guard, FEMA, and ICE were combined into one material weakness regarding *IT Controls and Financial System Functionality* for the FY 2015 DHS consolidated financial statements audit.

Specific results of testing of GITC, IT ELC, and IT application controls and non-technical information security at each DHS component were discussed with the appropriate members of management and communicated through Notices of Findings and Recommendations (NFRs). These test results are provided in separate, limited-distribution IT management letters to component management and the OIG.

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

FINDINGS AND RECOMMENDATIONS

Findings

We noted the following internal control weaknesses related to GITCs, IT ELCs, and IT application controls at the DHS components. Weaknesses indicated in this section represent a cross-representation of deficiencies identified at all components.

Deficiencies Related to IT Controls

Security Management

- Controls to monitor compliance with requirements for security awareness and role-based training for personnel with significant information security responsibilities were not always consistently implemented, and documentation of individuals required to take the role-based training was sometimes incomplete.

- Security authorization activities and supporting documentation and artifacts for core and feeder financial systems were not approved properly, updated timely, or documented accurately with respect to relevant system information.

- Plans of Action and Milestones (POA&Ms) were non-compliant with DHS policy, including no periodic review, no planned and completed milestones, planned corrective actions that were not detailed, expected completion dates in the past where weaknesses remained open, cancellation of POA&Ms despite remediation efforts that were still in progress, and POA&Ms that were not documented for known weaknesses.

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

Access Controls

- Policies and procedures for managing and monitoring access to key financial applications and underlying system software components, including those owned and operated by third-party service organizations on behalf of DHS and its components, were not consistently or completely developed and formally documented.

- Procedures for managing access to financial application, database, and operating system layers were not documented and implemented timely, or were not sufficiently detailed to identify and describe all application roles, including elevated privileges within the systems, or controls to review and authorize access to such privileges.

- Initial authorization, documentation, and periodic recertification of application, database, and operating system user, service, and generic accounts (including emergency and temporary access)

were inadequate, inconsistent, or in violation of the principles of least privilege and segregation of duties.

- Technical controls over logical access to key financial applications and underlying system software components and databases, including password requirements and account security configurations, were not consistently implemented in accordance with DHS requirements.

- Controls over the generation, review, analysis, and protection of application, database, and operating system audit logs were not fully implemented, or were inconsistently performed or not maintained by management.

- Access privileges of transferred and/or terminated employees and contractors were not always consistently or timely removed from financial systems and general support systems, and controls related to review and revocation of system access were not always implemented or finalized.

- Controls over the generation of complete and accurate listings of separated and/or terminated employees and contractors could not be produced.

Configuration Management

- Controls to validate the completeness and integrity of records regarding changes to key financial systems were not always implemented.

- Automated controls to detect, log, and maintain auditable records of all implemented changes to the applications and supporting system software to ensure that movements of code into the production environments were appropriately controlled and limited to authorized changes were not implemented.

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

- A process to comply with Information System Vulnerability Bulletin (ISVB) requirements or document waivers for non-compliant configurations had not been implemented.

- Certain configuration-related deficiencies were identified on servers and system software that were not remediated within a timely manner and tracked appropriately for remediation within management's POA&M.

- Configuration management policies and procedures for key financial systems were not always documented.

- A process to configure production client parameter settings had not been implemented.

Segregation of Duties

- Implementation of segregation of duties for IT and financial management personnel with access to financial systems across several platforms and environments (including development and production) was inadequate or incomplete.

Contingency Planning

- Service continuity plans were not always tested, and alternate processing sites were not always established for financial systems.

- A process had not been designed and implemented for performing daily system backups for the virtual application servers for the entire FY 2015 for one financial system.

IT Application Controls

- One component's primary financial system allowed obligations to be posted to future dates, which allowed receipts to be processed in excess of available funding, and payments to be processed against these obligations where there was no available funding.

- One component's 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.

Deficiencies Related to Financial Systems Functionality

In addition to the IT control deficiencies noted above, we identified many instances across all DHS components where financial system functionality limitations were inhibiting DHS's ability to implement and maintain internal control, including process-level IT application controls supporting financial data processing and reporting. Financial system functionality limitations also contributed to other control deficiencies and compliance findings presented in our *Independent Auditors' Report*. We noted persistent and pervasive financial system functionality limitations in the following general areas at multiple components:

- System software supporting key financial applications, feeder systems, and general support systems either lacked the required functionality to implement effective controls or were outdated and no longer supported by the respective vendors, resulting in unmitigated vulnerabilities that exposed underlying data to potential unauthorized and undetected access and exploitation.
- GITCs and financial process areas were implemented or supported by manual processes, outdated or decentralized systems or records management processes, or utilities with limited automated capabilities. These limitations introduced a high risk of error and resulted in inconsistent, incomplete, or inaccurate control execution and supporting documentation.

- Multiple components' financial system controls were not fully effective to efficiently provide readily auditable transaction populations without substantial manual intervention and additional supporting information, which increased the risk of error.

In addition to these general areas, system limitations contributed to deficiencies noted in multiple financial process areas across the DHS Components. For example, system configurations and posting logic deficiencies limited the effectiveness of controls to properly calculate the value of certain transactions, identify funding variances, or prevent or detect and correct excessive refund claims. In some cases, while Components implemented manual processes to compensate for these limitations, these manual processes were prone to error and increased the risk that financial data and transactions were improperly posted to the respective systems.

Cause

The control deficiencies described above stem from a number of systemic root causes across the affected DHS Components. In many cases, resource limitations, ineffective or inadequate management oversight, the complex, highly interrelated yet decentralized nature of systems and system components, or error-prone manual processes resulted in inadequately designed and implemented or ineffectively operating controls. In some cases, cost-prohibitive options for vendor support had limited system development activity to "break/fix" and sustainment activities.

Effect

DHS management continued to recognize the need to upgrade its financial systems. Until serious legacy IT issues are addressed and updated IT solutions are implemented, compensating controls and other complex manual workarounds must support the IT environment and financial reporting processes of DHS and its components'. As a result, DHS's difficulty attesting to a strong control environment, including effective general IT controls and reliance on key financial systems, will likely continue.

The conditions supporting our findings collectively limit DHS's ability to process, store, and report financial data in a timely manner to ensure accuracy, confidentiality, integrity, and availability. Some of the weaknesses may result in material errors in DHS's financial data that are not detected in a timely manner through the normal course of business. In addition, because of the presence of IT control and financial system functionality weaknesses, there is added pressure on mitigating controls to operate effectively. Because mitigating controls were often more manually focused, there was an increased risk of human error that could materially affect the financial statements.

Recommendation

We recommend that the DHS Office of the Chief Financial Officer (OCFO), in coordination with the Office of the Chief Information Officer (OCIO) and component management, continue the *Financial Systems Modernization* initiative and make necessary improvements to the Department's and components' financial management systems and supporting IT security controls. Specific, more detailed recommendations were provided in individual, limited distribution (For Official Use Only [FOUO]) NFRs and separate letters provided to DHS and component management.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY AWARENESS

To complement our IT controls test work during the FY 2015 audit, we performed additional non-technical information security procedures at certain DHS components. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where DHS component 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 DHS component personnel were willing to divulge network or system passwords that, if exploited, could compromise DHS or component sensitive information.

To conduct this testing, we made phone calls from various DHS locations at various times throughout the audit. Posing as component technical support personnel, we attempted to solicit access credentials from component users. Attempts to log into component systems were not performed; however, we assumed that disclosed passwords that met the minimum password standards established by DHS policy were valid exceptions. At seven of the nine components where social engineering was performed, we noted instances where individuals divulged passwords in violation of DHS policy.

Component	Number of Calls Attempted	Number of Individuals Reached	Number of Exceptions Noted
CBP	60	14	2
USCG	48	14	0
CIS	45	10	0
CONS	28	8	0
FEMA	45	12	1
ICE	45	10	2
MGT	45	13	3
TSA	45	9	3

The selection of attempted or connected calls was not statistically derived; therefore, the results described here should not be used to extrapolate to any component or the Department 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 DHS component 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 component 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 the component, DHS OIG, and DHS OCIO.

At each component where after-hours physical security walkthroughs were performed, we noted instances where 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 laptops, mobile devices, or storage media – was left unattended and unsecured after business hours in violation of DHS policy.

Component	Number of Workspaces Inspected	Number of Workspaces with Exceptions Noted
CBP	120	34
USCG	256	83
CIS	64	19
CONS	68	6
FEMA	198	53
ICE	84	36
MGT	28	12
TSA	56	24
USSS	42	22
MGT	28	12

The selection of inspected areas was not statistically derived; therefore, the results described here should not be used to extrapolate to any component or the Department as a whole.

MANAGEMENT RESPONSE

The DHS Office of Inspector General discussed our report with DHS management. The OIG reported that DHS management concurs with the findings and recommendations described in this letter and will continue to work with component management to address these issues.

Appendix A

Description of Key DHS Financial Systems and IT Infrastructure Within the Scope of the FY 2015 DHS Financial Statement Audit

Below is a description of significant DHS and component financial management systems and supporting IT infrastructure included in the scope of the DHS FY 2015 financial statement audit.

DHS Headquarters (Office of Financial Management / Office of the Chief Information Officer)

DHS Treasury Information Executive Repository (DHSTIER)

DHSTIER is the system of record for the DHS consolidated financial statements and is used to track, process, and perform validation and edit checks against monthly financial data uploaded from each of the DHS components' core financial management systems. DHSTIER is administered jointly by the OCFO Resource Management Transformation Office and the OCFO Office of Financial Management.

Customs and Border Protection (CBP)

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 a target completion date 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 the ACE with a target completion date 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 the 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) to transfer payroll-specific data for processing and eventual transmission to the USDA National Finance Center.

COSS is developed and maintained by the CBP BEMSD and the CBP OIT. The application is hosted and supported by the 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.

Time and Attendance Management System (TAMS)

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 the CBP BEMSD and the CBP Office of Information and Technology. The application is hosted and supported by the 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.

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 also 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 U.S. Department of the Treasury's (DoT) offices (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 the CBP BEMSD. The application is hosted and supported by the CBP OIT for internal use by the CBP user community, DOJ, and DoT.

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 information technology 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 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 the CBP CSPD and the EDMED, and hosted and supported by the 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 the 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 the CBP OIT exclusively for internal use by the CBP user community.

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

United States Coast Guard

Core Accounting System (CAS)

CAS is a web-based major application and the official accounting system of record for the Coast Guard. It is used to record all income and expenses and create income statements, balance sheets, and other financial reports to show financial condition. Accounting and financial management functions supported by CAS include accounts payable, accounts receivable, general and expense ledgers, and asset (including capital asset) management. It contains interfaces with DHS' Treasury Information Executive Repository, internal Coast Guard feeder systems, and external service providers (including the Department of Treasury's Bureau of the Fiscal Service).

The CAS application is an Oracle Federal Financials product with an Oracle database with Microsoft Windows-based and HP-UX (Hewlett-Packard UniX) and Red Hat UNIX-based servers.

CAS is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard user community. It is hosted by Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, Virginia.

Finance Procurement Desktop (FPD)

FPD is a web-based major application that supports Coast Guard funds management processes by creating and managing simplified procurement documents and maintaining accurate accounting records agency-wide. Functions performed by FPD include budgeting and funds distribution, procurement requests and simplified acquisitions, receipt of goods/services (accruals), and program element status reporting. It is integrated with CAS and contains interfaces with the DHS Treasury Information Executive Repository, other internal Coast Guard feeder systems (including the Contract Management Information System), and external service providers (including the Department of Treasury's Bureau of the Fiscal Service).

The FPD application is supported by an Oracle database with Microsoft Windows-based and HP-UX and Red Hat UNIX-based servers.

FPD is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard financial management and acquisitions user community. It is hosted by Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, Virginia.

Workflow Imaging Network System (WINS)

WINS is a web-based major application that supports the procurement process through the imaging and documenting of vendor invoices. Contracting Officers (KO) or representatives enter invoice data within the application that is interfaced to the Core Accounting System upon approval.

The WINS application is supported by an Oracle database with Microsoft Windows-based and HP-UX and Red Hat UNIX-based servers.

WINS is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard financial management and acquisitions user community. It is hosted by Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, Virginia.

Direct Access

The United States Coast Guard (USCG) Direct Access is an internet-accessible, web-based, USCG-wide, full-lifecycle military human resources (HR) and payroll solution using commercial/government off-the-shelf products from Oracle and PeopleSoft. It is hosted by a third-party application service provider and is maintained by a mix of government staff and contractor support. Direct Access is the primary system for HR and payroll for over 50,000 Coast Guard, Health and Human Services (HHS) Public Health Service (PHS), and National Oceanic and Atmospheric Administration (NOAA) active duty and reserve personnel. It also provides HR and pay support to a customer base of approximately 68,000 Coast Guard,

Health and Human Services (HHS), PHS, and National Oceanic and Atmospheric Administration (NOAA) retirees, annuitants, and Former Spouse Protection Act (FSPA) recipients, while providing non-pay customer service support to an additional 2,500 personnel. Direct Access provides military assignment processing, aids in the management of personnel housing and occupancy, supports recruitment and accession processes, posts official Coast Guard positions, schedules training, manages personnel assets and readiness, tracks and processes retirements, processes promotions and disciplinary actions, maintains all personnel attributes, and provides military payroll.

The Direct Access system runs on several Microsoft Windows-based and Red Hat-based UNIX servers. Separate development and test environments are maintained. Network Attached Storage (NAS) is used in combination with locally attached storage. The failover (disaster recovery) systems bear the virtually identical hardware configuration.

Direct Access has implemented applicable DHS Hardening Guidelines as well as applicable Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) (e.g., RedHat Linux, Oracle Database Management System (DBMS), VMWare, Windows 2008, etc.). The system has its own dedicated hardware and storage and the hosting provider is FEDRAMP certified.

Naval and Electronics Supply Support System (NESSS)

NESSS is a web-based major application that provides integrated provisioning and cataloging, unit configuration, supply and inventory control, procurement, depot-level maintenance, property accountability, and financial ledger capabilities as part of the family of Coast Guard logistics systems.

The Oracle Forms and Reports application is supported by an Oracle database with Microsoft Windows-based and Red Hat-based UNIX servers. In August 2015, the Coast Guard enabled the application for single sign-on capability.

NESSS is developed, maintained, and hosted by the Coast Guard Operations Systems Center (OSC) (a component of the Office of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology) in Kearneysville, West Virginia and managed by the Office of Logistics Information. It is supported by OSC exclusively for internal use by the Coast Guard Yard and the Surface Forces Logistics Center (SFLC) finance and logistics user communities.

Aviation Logistics Management Information System (ALMIS)

ALMIS is a hybrid web-based and client-server major application that provides Coast Guard aviation logistics management support in the areas of operations, configuration management, maintenance, supply, procurement, financial management, and business intelligence. It includes the inventory management and fiscal accounting functionality of the Aviation Maintenance Management System (AMMIS) subsystem to improve inventory purchase/repair decisions and provide total asset visibility. ALMIS supports data flight operations, flight execution recording, aircrew events tracking, aircraft aging, aircraft configuration management, aircraft maintenance, aircraft parts replacement, warehouse activities, procurement actions, financial payments, and reconciliation.

The application is supported by Ingres databases with HP-UX and Red Hat UNIX-based servers.

ALMIS is developed, maintained, hosted, and supported by the Coast Guard Aviation Logistics Center (ALC) in Elizabeth City, North Carolina and is exclusively for internal use by the Coast Guard financial management and aviation logistics user community.

National Pollution Funds Center (NPFC) Case Information Management System (CIMS)

NPFC-CIMS is one of four web-based major applications that comprise the Management and Operation Support Information Systems (MOSIS) suite. The application supports the NPFC's mission to manage the funding and prosecution of pollution cases (also known as projects). It provides the Coast Guard and Environmental Protection Agency (EPA) Federal On-Scene Coordinators (FOSCs) access to the Oil Spill Liability Trust Fund (OSLTF) or Comprehensive Environment Response, Compensation, and Liability Act (CERCLA) funds to respond to pollution incidents. CIMS consists of financial and non-financial case information, such as responsible party, pollution response status, costs, and accounts receivable. Projects within CIMS are first created and initiated via interfaces from NPFC's Ceiling and Number Assignment Processing System (CANAPS) and the Claims Processing System (CPS). Project costs are downloaded daily from the Core Accounting System's Mirror Database (CAS MIR).

The Oracle Financials application includes three modules – accounts receivable, project accounting, and general ledger. CIMS sits on an Oracle database with Red Hat UNIX-based servers supporting it.

The entire MOSIS suite of systems is housed by the Operations Systems Center (OSC) in Kearneysville, West Virginia. NPFC end-users reside throughout the country; however, program management is conducted out of Arlington, Virginia.

WebTA

WebTA is a commercial off-the-shelf (COTS) web-based major application hosted by the USDA National Finance Center (NFC) and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The Coast Guard utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the Coast Guard user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the USDA NFC and developed, operated and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

U.S. Citizenship and Immigration Services (USCIS)

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for USCIS. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

FFMS includes a back-office component used by the USCIS OCFO and the USCIS Financial Management Division. FFMS also includes a desktop application used by the broader USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center). The USCIS instance of FFMS contains no known internal or external interfaces.

The USCIS instance is hosted and supported by the ICE OCIO on behalf of USCIS (under the terms established through a Memorandum of Understanding between the two components), exclusively for internal use by the USCIS user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for USCIS.

The application is hosted at Datacenter 2 in Clarksville, VA and is supported by the IBM z/OS mainframe and Oracle databases.

Purchase Request Information System (PRISM)

PRISM is a contract writing system used by USCIS acquisition personnel to create contract awards. PRISM is interfaced with the Federal Procurement Data System – Next Generation. USCIS utilizes an instance of the application while the DHS Office of the Chief Procurement Officer (OCPO) owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

PRISM is supported by an Oracle database with UNIX-based servers. The system resides in Datacenter 1 in Stennis, Mississippi.

WebTA

WebTA is a COTS web-based major application hosted by the USDA National Finance Center (NFC) and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The USCIS Office of Human Capital and Training (OHCT) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the USCIS user community to facilitate payroll processing.

Electronic System for Personnel (ESP)

ESP is a web-based application used for Standard Form (SF)-52 processing. The ESP environment is hosted, operated, and maintained by ICE OCIO and used by multiple components.

Electronic Immigration System (ELIS2)

ELIS2 is a web-based application used by individuals to file their I-90 applications and make payments (such as filing fees, biometric services fees, and the USCIS Immigrant Fee) online. It also provides real-time case status updates to individuals seeking U.S. citizenship.

ELIS2 is supported by an Oracle database with Linux-based servers. The system resides on a Infrastructure as a Service (IaaS) private cloud at Amazon Web Services (AWS) Northern Virginia.

Federal Emergency Management Agency (FEMA)

Web Integrated Financial Management Information System (WebIFMIS)

WebIFMIS is a web-based major application and the official accounting system of record for FEMA. It maintains and is the source of all financial data for both internal and external financial reporting. It is comprised of five subsystems (Funding, Cost Posting, Disbursements, Accounts Receivable, and General Ledger) that budget, record, and track all financial transactions, manage vendor accounts, and process approved payments to grantees, FEMA employees, contractors, and other vendors.

WebIFMIS contains interfaces with internal FEMA feeder systems and external service providers, including the Department of Treasury's Bureau of the Fiscal Service, the USDA NFC, and the Department of Health and Human Services (HHS) Grants Management System.

WebIFMIS is a COTS software package developed and maintained by Digital Systems Group, Inc., and hosted and supported by the FEMA OCFO and FEMA OCIO exclusively for internal use by the OCFO user community.

WebIFMIS is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Payment and Reporting System (PARS)

PARS is a web-based major application that includes a public-facing component that collects quarterly SF 425 (Federal Financial Report) submissions and payment requests from grantees. Through daily automated scheduled jobs, grant and obligation information is updated via an interface between PARS and WebIFMIS. An internal component (OCFO) provides FEMA staff with the ability to view SF 425 submissions, examine grantee payment history reports, and add or remove holds on grantee payments.

PARS is hosted and supported by FEMA OCFO for external use by grantees and internal use by the OCFO user community.

PARS is supported by an Oracle database with HP-UX servers. The system resides in Mt. Weather, VA.

Non-Disaster Grant Management System (NDGrants)

NDGrants is a web-based major application intended to provide FEMA and its stakeholders with a system that supports the grants management lifecycle. FEMA provides state and local governments with preparedness program funding in the form of Non-Disaster Grants to enhance the capacity of state and local emergency responders to prevent, respond to, and recover from weapons of mass destruction terrorism incidents involving chemical, biological, radiological, nuclear, and explosive devices and cyber-attacks.

NDGrants includes a public-facing component that permits external grantees and stakeholders to apply for grants, monitor the progress of grant applications and payments, and view related reports. NDGrants also has an internal component used by the FEMA Grants Program Directorate (GPD), Program Support Division (PSD), to review, approve, and process grant awards. It contains an interface with the HHS Grants.gov system to facilitate upload and integration of information submitted via SF 424 (Application for Federal Assistance).

NDGrants is hosted and supported by FEMA GPD and FEMA OCIO for external use by grantees and stakeholders and internal use by the GPD user community.

NDGrants is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Assistance to Firefighters Grants (AFG)

AFG is a web-based major application developed to assist the United States Fire Administration (USFA) division of FEMA in managing the AFG program. The primary goal of AFG is to meet the firefighting and emergency response needs of fire departments, first responders, and nonaffiliated emergency medical service organizations to obtain equipment, protective gear, emergency vehicles, training, and other resources to protect the public and emergency personnel from fire and related hazards.

AFG includes a public-facing component that permits external grantees and stakeholders to apply for grants and submit payments and reports, and an internal component used by the GPD PSD and the AFG Program Office to review, approve, and process grant awards.

AFG is hosted and supported by FEMA GPD and FEMA OCIO for external use by grantees and stakeholders and internal use by the GPD user community.

AFG is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Emergency Management Mission Integrated Environment (EMMIE)

EMMIE is a web-based major application used by FEMA program offices and user communities directly involved in the grant lifecycles associated with the Public Assistance grant program. These include Fire

Management Assistance grants to provide assistance to State, Tribal, and local governments, and certain types of private nonprofit organizations so that communities can quickly respond to and recover from major disasters or emergencies declared by the President.

EMMIE includes a public-facing component that permits external grantees and stakeholders to apply for grants, and an internal component used by the different communities of interest involved in the successful processing of a grant from solicitation to closeout and assisting with coordination between the respective program and grants management offices and the Office of Legislative Affairs. The system also contains an interface with the Environmental and Historic Preservation Management Information System (EMIS) to automate the process of reviewing and documenting FEMA-funded projects for environmental and historic preservation (EHP) compliance.

EMMIE is hosted and supported by the FEMA Public Assistance Division (PAD) and the FEMA OCIO for external use by grantees and stakeholders and internal use by the FEMA user community.

EMMIE is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Emergency Support (ES)

ES is a web-based major application that performs front-end financial management for disaster processing and controls and monitors FEMA's funds and external financial interfaces. As a module of the National Emergency Management Information System (NEMIS), ES pre-processes financial transactions, including allocation, commitment, obligation, mission assignment, and payment requests from other NEMIS modules and other external systems and serves as the primary interface to WebIFMIS. ES supports the Enterprise Coordination and Approvals Processing System (eCAPS), which provides support to initiate, track, and expedite the process of providing direct aid and technical assistance, including electronic coordination and approval of internal requisitions for services and supplies, and mission assignments, to other Federal agencies and states in response to Presidentially-declared disasters.

ES includes a public-facing component that permits access for applicants for grants or disaster assistance and other state, local, and non-governmental organization (NGO) representatives and members of the public. It also includes an internal component used by FEMA OCFO to process disaster housing payments, perform payment recoupment, and conduct other administrative tasks associated with disaster payments.

In addition to WebIFMIS and eCAPS, ES contains interfaces with other internal FEMA feeder systems, including EMMIE and AFG.

ES is hosted and supported by the FEMA OCFO and FEMA OCIO for external use by grantees and stakeholders and internal use by the OCFO user community.

ES is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Transaction Recording and Reporting Processing (TRRP)

TRRP is a mainframe-based application and a subsystem of the National Flood Insurance Program (NFIP) Information Technology System (ITS) GSS that collects, maintains, and reports on all data and activity submitted by the Write Your Own (WYO) companies and the Direct Servicing Agent (DSA) for NFIP. Additionally, TRRP creates and updates policies, claims, and community master files that are maintained on the NFIP ITS mainframe.

TRRP is hosted and supported by Computer Sciences Corporation (CSC), Inc., on behalf of the Federal Insurance & Mitigation Administration, exclusively for internal use by the NFIP user community.

TRRP is supported by a FOCUS database with an IBM z/OS mainframe. The system resides in Norwich, CT.

Payment Management System (PMS)

The PMS, commonly referred to as Smartlink, is a web-based major application hosted, developed, operated, and maintained by the HHS National Institutes of Health (NIH) Center for Information Technology (CIT) Information Systems Branch (ISB). The FEMA OCFO's Finance Center user community uses Smartlink to disburse grant funds to grantees, track and maintain grantee payment and expenditure data, and manage cash advances to recipients.

PMS is supported by an Oracle database with HP-UX servers. The system resides in Bethesda, MD.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The FEMA Office of the Chief Component Human Capital Officer (OCCHCO) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the FEMA user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the NFC and developed, operated, and maintained by the NFC IT services division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Federal Law Enforcement Training Centers (FLETC)

Financial Accounting and Budgeting System (FABS)

FABS is a web-based major application and the official accounting system of record for FLETC. An instance of the COTS financial processing system known as Momentum, it is used to input requisitions, approve receipt of property, and manage property asset records and financial records for contracts, payments, payroll, and budgetary transactions. It contains interfaces with external service providers including the USDA NFC and the GSA Concur Government Edition (CGE) electronic travel system.

The application is supported by an Oracle database with Microsoft Windows-based and Red Hat UNIX-based servers.

FABS is physically hosted within Datacenter 1 in Stennis, Mississippi, and managed by a service provider who performs operating system administration. FLETC still performs database and application administration.

Purchase Request Information System (PRISM)

PRISM is a contract writing system used by FLETC acquisition personnel to create contract awards. PRISM is interfaced with the Federal Procurement Data System – Next Generation. FLETC utilizes an instance of the application while the DHS Office of the Chief Procurement Officer (OCPO) owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

PRISM is supported by an Oracle database with UNIX-based servers. The system resides in Datacenter 1 in Stennis, Mississippi.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and WebTA to process front-end input and certification of time and attendance entries by the DHS user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Immigration and Customs Enforcement (ICE)

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for ICE. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

FFMS includes a back-office component used by the ICE OCFO and the ICE Office of Financial Management. FFMS also includes a desktop application used by the broader ICE and USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center). The ICE instance of FFMS contains interfaces with internal ICE feeder systems and external service providers, including the Department of Treasury's Bureau of the Fiscal Service and the USDA NFC.

The ICE instance of FFMS is hosted and supported by the ICE OCIO, exclusively for internal use by the ICE user community. The USCIS instance is hosted and supported by the ICE OCIO on behalf of USCIS (under the terms established through a Memorandum of Understanding between the two components), exclusively for internal use by the USCIS user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for USCIS.

The application is hosted at Datacenter 2 in Clarksville, VA and is supported by the IBM z/OS mainframe and Oracle databases.

Bond Management Information System (BMIS)

The BMIS is an immigration bond management database used primarily by the Office of Financial Management (OFM) at ICE. The basic function of BMIS is to record and maintain for financial management purposes the immigration bonds that are posted for aliens involved in removal proceedings.

The application is hosted at Datacenter1 in Stennis, MS, and is supported by an Oracle database and Windows servers.

Real Property Management System (RPMS)

RPMS is an enterprise real estate system for tracking ICE's property portfolio. This includes capturing and generating data in order to create reports on projects, space and move management, leases and contracts, facilities operations and maintenance, energy and environmental, and geospatial information.

The application is hosted at Datacenter 1 in Stennis, MS, and is supported by an Oracle database and Windows servers.

Purchase Request Information System (PRISM)

PRISM is a contract writing system used by ICE acquisition personnel to create contract awards. PRISM is interfaced with the Federal Procurement Data System – Next Generation. ICE utilizes an instance of the application while the DHS Office of the Chief Procurement Officer (OCPO) owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

PRISM is supported by an Oracle database with UNIX-based servers. The system resides in Datacenter 1 in Stennis, Mississippi.

WebTA

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The ICE Office of the Human Capital Officer (OHC) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the ICE user community to facilitate payroll processing.

Management Directorate (MGMT)

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for the DHS Management Directorate. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

The DHS Management Directorate instance of FFMS is hosted and supported by the ICE OCIO, exclusively for internal use by the DHS Management Directorate user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for the DHS Management Directorate.

The application is hosted at Datacenter 2 in Clarksville, VA, and is supported by the IBM z/OS mainframe and Oracle databases.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The DHS Office of Human Capital (OHC) utilizes NFC and WebTA to process the front-end input and certification of time and attendance entries by the DHS Management Directorate user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT services division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize and send personnel data to NFC for processing.

National Protection and Programs Directorate (NPPD)

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for NPPD. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

The various instances of FFMS that NPPD uses are hosted and supported by the ICE OCIO on behalf of NPPD, exclusively for internal use by the NPPD user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for NPPD.

The application is hosted at Datacenter 2 in Clarksville, VA, and is supported by the IBM z/OS mainframe and Oracle databases.

Science and Technology Directorate (S&T)

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for S&T. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

The S&T instance of FFMS is hosted and supported by the ICE OCIO, exclusively for internal use by the S&T user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for S&T.

The application is hosted at Datacenter 2 in Clarksville, VA and is supported by the IBM z/OS mainframe and Oracle databases.

Transportation Security Administration (TSA)

Core Accounting System (CAS)

CAS is a web-based major application and the official accounting system of record for TSA. It is used to record all income and expenses and create income statements, balance sheets, and other financial reports to show financial condition. Accounting and financial management functions supported by CAS include accounts payable, accounts receivable, general and expense ledgers, and asset (including capital asset) management. It contains interfaces with internal TSA feeder systems and external service providers,

including the Department of Treasury's Bureau of the Fiscal Service. It is hosted by the Coast Guard at Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, VA.

The CAS application is an Oracle Federal Financials product with an Oracle database with Microsoft Windows-based and HP-UX and Red Hat UNIX-based servers.

CAS is hosted and supported by the Coast Guard Office of the Director of Financial Operations/Comptroller and the Coast Guard OCIO on behalf of TSA (under the terms established through an interagency agreement between the two Components). It is exclusively for internal use by the TSA user community and, on a limited basis, Coast Guard personnel performing support services for TSA.

Finance Procurement Desktop (FPD)

FPD is a web-based major application that supports TSA funds management processes by creating and managing simplified procurement documents and maintaining accurate accounting records agency-wide. Functions performed by FPD include budgeting and funds distribution, procurement requests and simplified acquisitions, receipt of goods/services (accruals), and program element status reporting. It is integrated with CAS and contains interfaces with other internal TSA feeder systems, including the Contract Management Information System, and external service providers such as the Department of Treasury's Bureau of the Fiscal Service.

The FPD application is supported by an Oracle database with Microsoft Windows-based and HP-UX and Red Hat UNIX-based servers.

FPD is hosted and supported by the Coast Guard Office of the Director of Financial Operations/Comptroller and the Coast Guard OCIO on behalf of TSA (under the terms established through an interagency agreement between the two Components). It is exclusively for internal use by the TSA financial management and acquisitions user community and, on a limited basis, Coast Guard personnel performing support services for TSA. It is hosted by the Coast Guard at Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, VA.

Sunflower Asset Management System

Sunflower is a web-based application used by TSA for property management. It is comprised of modules including the management of inventory assets, excess assets, agreement assets, and inactive assets, and is integrated with FPD and the fixed assets module within CAS to create assets from purchase orders or receipts.

The Sunflower application is supported by an Oracle database with Microsoft Windows-based and HP-UX and Red Hat UNIX-based servers.

Sunflower is hosted and supported by the Coast Guard Office of the Director of Financial Operations/Comptroller and the Coast Guard OCIO on behalf of TSA (under the terms established through an interagency agreement between the two Components). It is exclusively for internal use by the

TSA financial management and property management user community. It is hosted by the Coast Guard at Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, VA.

MarkView

MarkView is a web-based application used by TSA to manage invoice imaging and workflow activities and interfaces with the accounts payable module within CAS.

The Markview application is supported by an Oracle database with Microsoft Windows-based and HP-UX and Red Hat UNIX-based servers.

MarkView is hosted and supported by the Coast Guard Office of the Director of Financial Operations/Comptroller and the Coast Guard OCIO on behalf of TSA (under the terms established through an interagency agreement between the two Components). It is exclusively for internal use by the TSA financial management and procurement user community and Coast Guard Finance Center support personnel. It is hosted by the US Coast Guard at Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, VA.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and WebTA to process the front-end input and certification of time and attendance entries by the DHS user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the NFC and developed, operated, and maintained by the NFC IT services division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

United States Secret Service (USSS)

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and WebTA to process front-end input and certification of time and attendance entries by the DHS user community to facilitate payroll processing.

Appendix B

FY 2015 IT Notices of Findings and Recommendations at DHS

Office of Financial Management (OFM) / Office of the Chief Information Officer (OCIO)

FY 2015NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at OFM	Security Management		X

Customs and Border Protection (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

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-15-11	Security Awareness Issues Identified during Social Engineering Testing at Customs and Border Protection (CBP)	Security Management		X
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	

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-15-22	Weakness in Human Resources Business Engine (HRBE) Database (DB) Access Provisioning Process	Access Controls	X	
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

United States Coast Guard (USCG)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-15-01	Weakness in NESSS Operating System Account Recertification	Access Controls	X	
CG-IT-15-02	Weakness in NPFC Operating System Account Recertification	Access Controls	X	
CG-IT-15-03	Lack of Approval Over Shared Account Usage for NPFC and NESSS OS Accounts	Access Controls	X	
CG-IT-15-04	Naval and Electronics Supply Support System (NESSS) Database Profile Security Configurations	Access Controls		X
CG-IT-15-05	Inappropriate NESSS Database Accounts Exist Due to a Lack of an Account Recertification Process	Access Controls	X	
CG-IT-15-06	Weakness in NPFC Database Security Configurations	Access Controls	X	
CG-IT-15-07	Lack of Consistent Contractor, Civilian, and Military Account Termination Process	Access Controls		X
CG-IT-15-08	Lack of Approval Over Shared Account Usage for NESSS Database Accounts	Access Controls	X	
CG-IT-15-09	Security Awareness Issues Related to Physical Security	Security Management		X
CG-IT-15-10	Lack of Processes and Documentation in Place for NPFC Database Account Management	Access Controls	X	
CG-IT-15-11	Weakness in Direct Access Database Account Recertification	Access Controls	X	
CG-IT-15-12	Weakness in Direct Access Database Security Configurations	Access Controls		X
CG-IT-15-13	Lack of Approval Over Shared Account Usage for a NPFC CIMS PA Application Account	Access Controls	X	

CG-IT-15-14	Lack of Segregation of Duties within the Worfkflow Imaging Network System (WINS)	Segregation of Duties	X	
CG-IT-15-15	Security Management and Configuration Management Controls - Vulnerability Assessment	Configuration Management		X

United States Citizenship and Immigration Services (USCIS)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-15-02	Inadequate Account Management Procedural Documentation for the Electronic Immigration System (ELIS2) Environment	Access Controls	X	
CIS-IT-15-03	Inconsistent Implementation of Entity Level Account Recertification Management Directive for the Federal Financial Management System (FFMS)	Access Controls	X	
CIS-IT-15-04	Lack of ESP User Access Forms	Access Controls	X	
CIS-IT-15-05	Lack of WebTA User Access Forms	Access Controls	X	

Federal Emergency Management Agency (FEMA)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-15-01	Non-Compliance with DHS Secure Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls		X
FEMA-IT-15-02	Inconsistent Implementation of WebIFMIS and PARS Audit Log Controls	Access Controls		X
FEMA-IT-15-03	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the WebIFMIS and PARS Production Environments	Configuration Management		X
FEMA-IT-15-04	Lack of Automated Controls to Log Changes Deployed to Production for the EMMIE, the NDG, the ES, and the AFG Systems	Configuration Management		X
FEMA-IT-15-05	Insufficient Audit Log Controls for Key Financial Systems	Access Controls		X
FEMA-IT-15-06	Inconsistent Delegation of Authority and Authorization of Privileged Access for Systems Managed by OCIO IT Operations	Access Controls		X
FEMA-IT-15-07	NACS Account Management Weaknesses	Access Controls	X	
FEMA-IT-15-08	Non-Compliance with Alternative Processing Site Requirements for Key Financial Systems	Contingency Planning		X
FEMA-IT-15-09	Security Awareness Issues Identified during Social Engineering Testing at FEMA	Security Management		X
FEMA-IT-15-10	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-15-11	Non-Compliant Security Authorization Packages for Key Financial Systems	Security Management		X

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-15-12	Lack of Web Time and Attendance (WebTA) Account Management Policies and Procedures	Access Controls		X
FEMA-IT-15-13	Incomplete Implementation of Role-Based Training for Individuals with Significant Information Security	Security Management		X
FEMA-IT-15-14	Incomplete Documentation of Web Integrated Financial Management Information System (WebIFMIS) Application Functions	Access Controls and Segregation of Duties		X
FEMA-IT-15-15	Lack of Smartlink Account Management Policies and Procedures	Access Controls		X
FEMA-IT-15-16	Weaknesses Identified Through Vulnerability Management Procedures on Financially Significant Segments of the FEMA Enterprise Network (FEN) and End-User Computing Environment	Configuration Management		X
FEMA-IT-15-17	Non-Compliant Plan of Action and Milestone (POA&M) reporting for Key Financial Systems	Security Management	X	
FEMA-IT-15-18	Inconsistent Implementation of EmpowHR Account Management Controls	Access Controls	X	

Federal Law Enforcement Training Center (FLETC)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-15-01	Weakness in Momentum Database Security Configurations	Access Controls	X	
FLETC-IT-15-02	Inappropriate Access to the FABS Operating System	Access Controls	X	
FLETC-IT-15-03	Weakness in FABS Database Account Recertification	Access Controls	X	
FLETC-IT-15-04	Security Management and Configuration Management Controls-Vulnerability Assessment	Configuration Management	X	

United States Immigration and Customs Enforcement (ICE)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-IT-15-02	Security Awareness Issues Identified during Social Engineering Testing at ICE	Security Management	X	
ICE-IT-15-03	Real Property Management System (RPMS) Account Management Weakness	Access Controls	X	
ICE-IT-15-04	Lack of Bond Management Information System (BMIS) Configuration Management Plan	Configuration Management	X	
ICE-IT-15-05	Deficiency in ICE Federal Financial Management System (FFMS) User Account Authorization Process	Access Controls		X
ICE-IT-15-06	FFMS Application Control Failures	Business Process	X	
ICE-IT-15-07	Deficiency in ICE Web Time and Attendance (WebTA) User Account Authorization Process	Access Controls	X	

Management Directorate (MGT)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
MGT -IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at MGT	Security Management		X
MGT -IT-15-02	Security Awareness Issues Identified during Social Engineering Testing at MGT	Security Management		X
MGT -IT-15-03	Inability to Generate a Complete and Accurate Listing of Separated Contractors	Access Controls	X	
MGT -IT-15-04	Deficiency in MGT Web Time and Attendance (WebTA) User Account Authorization Process	Access Controls	X	
MGT -IT-15-05	Deficiency in EmpowHR User Account Authorization Process	Access Controls	X	

National Protection and Programs Directorate (NPPD)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
NPPD-IT-15-01	Inability to Generate a Complete and Accurate Listing of Separated Contractors	Access Controls	X	

Science and Technology Directorate (S&T)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ST-IT-15-01	Weakness in S&T FFMS User Separation Process	Access Controls	X	

Transportation Security Administration (TSA)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-15-01	Security Awareness Issues Identified During After-Hours Physical Security Testing at TSA	Security Management		X
TSA-IT-15-02	Security Awareness Issues Identified During Social Engineering Testing at TSA Headquarters	Security Management		X
TSA-IT-15-03	Inappropriate Access to the TSA Financial Data Warehouse	Access Controls	X	

United States Secret Service (USSS)

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
USSS-IT-15-01	Security Awareness Issues Identified During After-Hours Physical Security Testing at USSS	Security Management		X
USSS-IT-15-02	WebTA Account Management Policies and Procedures	Access Controls	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

Management Directorate

Deputy Under Secretary
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