OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the FY 2016 Department of Homeland Security Financial Statement Audit

Homeland Security

April 28, 2017
OIG-17-54

DHS OIG HIGHLIGHTS

Information Technology Management Letter for the FY 2016 Department of Homeland Security Financial Statement Audit

April 28, 2017

Why We Did This Audit

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

What We Recommend

We recommend the Acting 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, 2016. 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 fiscal year (FY) 2015. However, new findings noted in FY 2016: (1) relate to controls that were effective in prior years, (2) were control deficiencies for new systems similar to deficiencies previously reported, or (3) were controls that were not tested in FY 2015.

Most 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. In addition, certain of these deficiencies adversely impacted the internal controls over DHS' financial reporting and operations and therefore are considered to collectively represent a material weakness identified in the FY 2016 DHS Agency Financial Report.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 28, 2017

MEMORANDUM FOR: Jeanne Etzel
Acting Chief Information Officer

Stacy Marcott
Acting Chief Financial Officer

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

SUBJECT: *Information Technology Management Letter for the FY 2016 Department of Homeland Security Financial Statement Audit*

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

The independent public accounting firm KPMG LLP conducted the audit of DHS' FY 2016 financial statements and is responsible for the attached information technology management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control, nor do we provide conclusions on compliance with laws and regulations. We will post the final report on our website.

Please call me with any questions, or your staff may contact Kevin Burke, Acting Director, Information Systems and Acquisitions Division, at (202) 254-5451.

Attachment

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

December 15, 2016

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

Ladies and Gentlemen:

We planned and performed 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, 2016, 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. We also 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 its components' financial systems, we noted certain deficiencies in the general IT control areas of security management, access controls, configuration management, segregation of duties, and contingency planning. We also noted 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 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 in which 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* section of this letter.

We have provided a description of key DHS and component financial systems and IT infrastructure within the scope of the Fiscal Year 2016 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' organization gained during our work to make comments and suggestions that we hope will be useful.

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

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

DHS' response to the deficiencies identified in our audit is described on page13 of this letter. DHS' 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, 2016

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, 2016, (referred to herein as the "fiscal year (FY) 2016 financial statements"). In connection with our audit of the FY 2016 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITC), IT entity-level controls (ELC), 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 U.S. Government Accountability Office (GAO) issued the *Federal Information System Controls Audit Manual* (FISCAM), which formed the basis for our GITC and IT ELC evaluation procedures.

FISCAM was designed to inform financial statement auditors about IT controls and related audit concerns, to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial statement audit. It also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs, IT ELCs, and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs, IT ELCs, and the IT environment:

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

Although each of these FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs 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 2016 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 operating effectively, we tested selected IT application controls (process-level controls — fully automated or manual with an automated component) on financial systems and applications to assess internal controls over input, processing, and output of financial data and transactions.

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

Financial System Functionality

In recent years, we have noted that limitations in 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 2016, we continued to evaluate and consider the impact of financial system functionality on internal control over financial reporting.

Non-Technical Information Security Testing

To complement our IT controls test work, we conducted limited after-hours physical security testing and social engineering at selected 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 2016 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 2016 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2016 assessment of GITCs, IT ELCs, and IT application controls, we noted that although DHS made some progress in remediating IT findings we reported in FY 2015, new findings were noted in FY 2016. Some of the new findings related to controls that were effective in prior years, control deficiencies noted over new systems that were similar to deficiencies previously reported, or controls that were not tested in FY 2015.

The majority of the deficiencies that our audit identified were related to noncompliance with financial system controls. According to DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, and National Institute of Standards and Technology guidance, components' financial system controls lacked proper documentation; were not fully designed and implemented; were inadequately detailed; and were inconsistently implemented. The most significant weaknesses from a financial statement audit perspective continue to include, as reported in 2015:

1. excessive, unauthorized, or inadequately monitored access to, and activity within, key DHS financial applications and their supporting databases and operating systems;
2. configuration management controls that were not fully defined, followed, or effective; and
3. a 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' 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 deficiencies adversely impacted the internal controls over DHS' 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. These deficiencies were combined into one material weakness regarding *Information Technology Controls and Financial System Functionality* for the FY 2016 DHS consolidated financial statements audit.

Specific test results of GITC, IT ELC, 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 (NFR). These test results are provided in separate, limited-distribution IT management letters to component management and the OIG.

Although the recommendations we made should be considered by DHS, it is ultimately the responsibility of DHS and its 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 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.

- Plans of Action and Milestones (POA&Ms) were non-compliant with DHS policy, including no planned and completed milestones, planned corrective actions that were not detailed, cancellation of POA&Ms despite remediation efforts that were still in progress, expected completion dates that were not achievable within the timeline provided for actions needed, management's review of POA&Ms not being sufficient, and POA&Ms that were not documented for known weaknesses.

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 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 those owned and operated by third-party service organizations on behalf of DHS and its components, 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 documented and/or implemented in accordance with DHS requirements.

- Policies and procedures were not formally documented and 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.

- Controls over the use of generic user IDs, and/or shared accounts and shared passwords were not enforced to ensure that users were uniquely identified and authenticated.

- 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.

- The generation of complete and accurate listings of separated and/or terminated contractors could not be produced.

- Authority to approve privileged access had not been formally delegated by the appropriate party in compliance with DHS policy.

Configuration Management

- Configuration management policies and procedures for key financial systems were not always documented or were in draft for a portion of FY 2016.

- Configuration changes were not always authorized and approved prior to implementation in the production environment.

- Test plans and test results for configuration changes were not formally documented.

- Segregation of duties over program libraries was not always enforced.

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

- Vulnerability scans were not performed on a monthly basis as required by component policy.

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

- An effective process to successfully perform and retain weekly backups was not implemented.

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

IT Application Controls

- 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 instances across all DHS components in which financial system functionality limitations were inhibiting DHS' 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 DHS components. For example, system configurations and posting logic deficiencies limited the effectiveness of controls to properly calculate the value of certain transactions, to identify funding variances, or to prevent or detect and correct excessive refund claims. In some cases, even though 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.

Causes

The control deficiencies described in this Exhibit stem from a number of systemic root causes across the Department that resulted in inadequately designed and implemented or ineffectively operating controls, including:

- resource limitations
- ineffective or inadequate management oversight, awareness, and training
- reduced efforts to remediate legacy system processes due to competing priorities related to the modernization of the financial information system
- complex, highly interrelated, yet decentralized systems and system components
- a lack of communication between offices in the same organization regarding GITC ownership
- a lack of continual self-review and risk assessments performed for GITCs
- error-prone manual processes.

In some cases, cost-prohibitive options for vendor support limited system development activity to "break/fix" and sustainment activities.

Effect

Deficiencies related to access controls and segregation of duties increase the risk that current employees, separated employees, and contractors may obtain unauthorized or inappropriate access to financial and support systems or data. Such access could lead to unauthorized activities or inappropriate disclosures of sensitive data. Deficiencies related to configuration management increase the risk that unauthorized or inappropriate changes to systems will be applied and go undetected by management, resulting in lower assurance that information systems will operate as intended and that data is reliable, valid, and complete.

The conditions supporting our findings collectively limit DHS' ability to process, store, and report financial data in a timely manner that ensures accuracy, confidentiality, integrity, and availability. Some of the weaknesses could result in material errors in DHS' financial data that are not detected in a timely manner through the normal course of business. Because of the presence of IT control and financial system functionality weaknesses, there is added pressure on mitigation controls to operate effectively. Such mitigating controls often were not implemented. However, when implemented, mitigating controls often were more manually focused, increasing the risk of human error that could materially affect the financial statements. Furthermore, due to these GITC deficiencies, we were unable to rely on application controls

and information produced by the entity and used by management in the operation of certain key manual controls throughout the Department.

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' difficulty attesting to a strong control environment, including effective general IT controls and reliance on key financial systems, will likely continue.

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 2016 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 in which 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 2016 STAL signed by DHS OIG management, KPMG management, and DHS management.

Social Engineering

Social engineering is defined as the act of manipulating people into performing actions or divulging sensitive information. The term typically applies to trickery or deception for the purpose of gathering information or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which 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 two of the seven components where social engineering was performed, we noted instances in which individuals divulged passwords in violation of DHS policy.

Component	Number of Calls Attempted	Number of Individuals Reached	Number of Exceptions Noted
CBP	60	4	0
USCG	45	39	0
CIS	45	18	0
ICE	45	12	1
MGT	45	8	0
TSA	71	32	0
USSS	33	11	2

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 2016. We inspected workspaces to identify instances in which 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 in which material was left unattended and unsecured after business hours in violation of DHS policy. The instances include, but are 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.

Component	Number of Workspaces Inspected	Number of Workspaces with Exceptions Noted
CBP	120	32
USCG	326	59
CIS	70	8
CONS	69	3
FEMA	251	33
ICE	104	18
Management Directorate	63	6
TSA	51	6
USSS	55	19

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 OIG 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 2016 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 2016 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. The OCFO's Resource Management Transformation Office and Office of Financial Management jointly administer DHSTIER.

Procurement Request Information System Management (PRISM)

PRISM is a major application that the DHS Office of the Chief Procurement Officer (OCPO) hosts. PRISM provides comprehensive, Federal Acquisition Regulation (FAR)-based acquisition support for multiple DHS entities.

An Oracle database with UNIX-based servers supports PRISM, and the system resides in Datacenter 1 in Stennis, MS.

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 target completion by early calendar year 2017.

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

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

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

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

Automated Commercial System (ACS)

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

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

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

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

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

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

SAP ECC is a client/server-based major application, with configurable web access, and the official accounting system of record/general ledger for CBP. It is an integrated financial management system used to account for assets (e.g., budget, logistics, procurement, and related policy) and revenue (e.g., accounting and commercial operations including trade, tariff, and law enforcement), and to provide information for strategic decision making. CBP's SAP instance includes several modules that provide system functionality for funds management, budget control, general ledger, real estate, property, internal orders, sales and distribution, special purpose ledger, and accounts payable activities, among others. Data resulting from transactions that SAP ECC processes interfaces with SAP BW, which is optimized for query and report generation.

SAP contains interfaces with internal CBP feeder systems, including ACE, ACS, and external service providers, including the General Services Administration's (GSA) Next Generation Federal Procurement

Data System, U.S. Department of the Treasury's Bureau of the Fiscal Service, and FedTraveler.com's E-Gov Travel Service (ETS).

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

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

CBP Overtime Scheduling System (COSS)

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

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

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

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

Time and Attendance Management System (TAMS)

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

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

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

Seized Asset and Case Tracking System (SEACATS)

SEACATS is a mainframe-based application that enables the computerized tracking of all assets seized during CBP enforcement operations from the point when the asset is physically seized to the point when the asset is liquidated or related fines and penalties have been satisfied. In addition to tracking inventory,

SEACATS serves as a repository for all case notes produced through the administrative and judicial processes related to the prosecution of seized asset offenses and the disposition of the involved assets.

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

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

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

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

Real Time Online Source Code Editor (ROSCOE)

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

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

CA Top Secret Security (TSS) Managed Mainframe Environment

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

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

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

Human Resource Business Engine (HRBE)

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

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

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

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

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

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

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

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

United States Coast Guard

Core Accounting System (CAS)

CAS is a web-based major application and the official accounting system of record for the United States Coast Guard (USCG). 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. CAS interfaces with DHS' Treasury Information

Executive Repository, internal Coast Guard feeder systems, and systems of external service providers (including the Department of Treasury's Bureau of the Fiscal Service).

CAS is an Oracle Federal Financials product, including an Oracle database with HP-UX (Hewlett-Packard Unix)-based servers.

The Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO host and support CAS exclusively for the internal Coast Guard user community. The Operations Systems Center (OSC) Detachment Chesapeake, in Chesapeake, VA, hosts the application.

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. FPD is integrated with CAS and interfaces with the DHS Treasury Information Executive Repository, other internal Coast Guard feeder systems (including the Contract Management Information System), and systems of external service providers (including the Department of Treasury's Bureau of the Fiscal Service).

An Oracle database with HP-UX-based servers supports the FPD application.

The Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO host and support CAS exclusively for the internal Coast Guard user community. The OSC Detachment Chesapeake in Chesapeake, VA, hosts the application.

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 Contracting Officer Representatives (COR) enter invoice data within the application that interfaces with the Core Accounting System upon approval.

An Oracle database with HP-UX-based servers supports the WINS application.

The Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO host and support WINS exclusively for the internal Coast Guard financial management and acquisitions user community. The OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

Direct Access

The Coast Guard's Direct Access is an internet-accessible, web-based, agency-wide, full-lifecycle military human resources (HR) and payroll solution using commercial/government off-the-shelf products from Oracle and PeopleSoft. A third-party application service provider hosts the application, and a mix of

government and contractor staff support and maintain it. Direct Access is the primary system for HR and payroll for more than 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, HHS, PHS, and 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.

Direct Access runs on several Microsoft Windows-based and Red Hat-based UNIX servers, and Oracle databases support it.

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

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.

An Oracle database with Microsoft Windows-based and Red Hat-based Linux servers support this Oracle Forms and Reports application. In August 2015, the Coast Guard enabled the application for single sign-on capability.

The Coast Guard OSC (a component of the Office of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology) in Kearneysville, WV, developed, maintains, and hosts NESSS. The Office of Logistics Information manages the application. OSC supports the application exclusively for the internal Coast Guard Yard and 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 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.

Ingres and Oracle databases with Microsoft Windows, and HP-UX and Red Hat Linux-based servers support this application.

The Coast Guard's Aviation Logistics Center (ALC) in Elizabeth City, North Carolina, developed, maintains, hosts, and supports ALMIS exclusively for the internal Coast Guard financial management and aviation logistics user community.

National Pollution Funds Center's (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 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).

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

The OSC in Kearneysville, WV, hosts the entire MOSIS suite. NPFC end-users reside throughout the country; however, program management is conducted out of Arlington, VA.

Shore Asset Management (SAM)

SAM provides core information about the USCG shore facility assets and facility engineering. The application tracks activities and assists in the management of the Civil Engineering (CE) and Facility Engineering (FE) programs. SAM data contributes to shore facility assets full life cycle program management, and facility engineering full life cycle program management and rationale to adjust Coast Guard mission needs through planning, budgeting, and project funding. SAM also provides real property inventory and management of all shore facilities, in addition to the ability to manage and track facilities engineering equipment and the maintenance of that equipment.

Oracle databases with Microsoft Windows servers support SAM.

The OSC in Kearneysville, WV, hosts SAM.

Contract Information Management System (CIMS)

CIMS is a contract management system that is used for contract creation and management. It includes milestone planning, solicitations, award, and closeout. CIMS interfaces with FPD to receive commitments and send contract procurement information. The primary users of CIMS are contracting officers and contracting specialists.

Oracle databases with Microsoft Windows servers support CIMS. The OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

Open Obligation Validation Application (OOVA)

OOVA is a tool that enables financial managers to monitor and validate open obligations in accordance with DHS and Coast Guard policies. OOVA opens obligations from CAS and provides an instrument to classify each open obligation as to whether it is valid.

A Microsoft SQL Server and Microsoft Windows servers support OOVA. The OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

CAS Mirror Data Warehouse (MIR)

MIR is a direct copy (mirrored image) of the CAS production database and is used for reporting purposes. MIR is refreshed daily with the previous day's production data.

Oracle databases and Red Hat Linux-based servers support MIR. The OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

Coast Guard Business Intelligence (CGBI)/Enterprise Data Warehouse (EDW)

CGBI/EDW is a Business Intelligence (BI) and mission support tool that provides users with web-based reporting and analysis capability by using standardized enterprise data and metrics.

Oracle databases and Microsoft Windows and Red Hat Linux-based servers support CGBI/EDW. The OSC in Kearneysville, WV, hosts the application.

Web Time and Attendance (WebTA)

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

EmpowHR

EmpowHR is a COTS web-based major application that the USDA NFC hosts. The NFC IT Services Division and NFC Risk Management Staff developed, operate, and maintain the application. DHS components use 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 that USCIS OCFO and the USCIS Financial Management Division use. FFMS also includes a desktop application that the broader USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center) use. The USCIS instance of FFMS contains no known internal or external interfaces.

ICE OCIO on behalf of USCIS (under the terms of a Memorandum of Understanding established between the two components) hosts and supports the USCIS instance. This is done exclusively for the internal USCIS user community and, on a limited basis, for ICE OCIO and finance center personnel performing support services for USCIS.

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

PRISM

PRISM is a contract writing system that USCIS acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation. USCIS uses an instance of the application, and the DHS OCPO owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

An Oracle database with UNIX-based servers supports PRISM. The system resides in Datacenter 1 in Stennis, MS.

Electronic System for Personnel (ESP)

ESP is a web-based application used for Standard Form (SF)-52 processing.

ICE OCIO hosts, operates, and maintains the ESP environment, and many components use it. An Oracle database and Windows servers support the application, and it resides in Datacenter 1 in Stennis, MS.

Electronic Immigration System (ELIS2)

ELIS2 is a web-based application that individuals use 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.

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

WebTA

WebTA is a COTS web-based major application that the USDA NFC hosts. The NFC's IT Services Division and Risk Management Staff developed, operate, and maintain the application. The USCIS Office of Human Capital and Training (OHCT) uses NFC and WebTA to process front-end input and certification of USCIS user community time and attendance entries to facilitate payroll processing.

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 comprises 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, USDA's National Finance Center (NFC), and HHS' Grants Management System.

WebIFMIS is a COTS software package that Digital Systems Group, Inc. developed and maintains. FEMA's OCFO and OCIO host and support the application exclusively for the internal OCFO user community.

An Oracle database with Linux servers supports WebIFMIS, and 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 Standard Form (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.

FEMA OCFO hosts and supports PARS externally for grantees and internally for the OCFO user community.

An Oracle database with HP-UX servers supports PARS, and 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 that the FEMA Grants Program Directorate (GPD), Program Support Division (PSD) uses to review, approve, and process grant awards. NDGrants interfaces with the HHS Grants.gov system to facilitate upload and integration of information submitted via SF 424 (Application for Federal Assistance).

FEMA's GPD and OCIO host and support NDGrants externally for grantees and stakeholders, and internally for the GPD user community.

An Oracle database with Linux servers supports NDGrants, and 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.

FEMA GPD and FEMA OCIO host and support AFG externally for grantees and stakeholders, and internally for the GPD user community.

An Oracle database with Linux servers supports AFG, and 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 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 that different communities use when processing grants 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.

FEMA's Public Assistance Division (PAD) and OCIO host and support EMMIE externally for grantees and stakeholders, and internally for the FEMA user community.

An Oracle database with Linux servers supports EMMIE, and 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 helps initiate, track, and expedite the process of providing direct aid and technical assistance. This includes electronic coordination and approval of internal requisitions for services, supplies, and mission assignments to other Federal agencies and states in response to Presidentially-declared disasters.

ES includes a public-facing component that authorizes access to applicants for grants or disaster assistance, and to other state, local, and non-governmental organization (NGO) representatives and members of the public. It also includes an internal component that FEMA OCFO uses 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.

FEMA's OCFO and OCIO host and support ES externally for grantees and stakeholders, and internally for the OCFO user community.

An Oracle database with Linux servers support ES, and 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) general support system. It collects, maintains, and reports on all data and activity that the Write Your Own (WYO) companies and the Direct Servicing Agent (DSA) for NFIP submit. Additionally, TRRP creates and updates policies, claims, and community master files that are maintained on the NFIP ITS mainframe.

Computer Sciences Corporation (CSC), Inc. hosts and supports TRRP, on behalf of the Federal Insurance & Mitigation Administration, exclusively for the NFIP user community.

A FOCUS database with an IBM z/OS mainframe supports TRRP, and the system resides in Norwich, CT.

Quick Claims

Quick Claims is a web-based application that a Windows operating system and MySQL database support. WYOs use the application to self-report claims data prior to officially submitting that data through TRRP. The NFIP Actuary incorporates September claims data per Quick Claims into its actuarial calculation, as September claims data is not available from TRRP until after financial reporting deadlines for year-end. The system resides in Norwich, CT.

Payment Management System (PMS)

PMS, commonly referred to as Smartlink, is a web-based major application that the HHS National Institutes of Health's (NIH) Center for Information Technology (CIT) Information Systems Branch (ISB) developed, hosts, operates, and maintains. 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. An Oracle database with HP-UX servers supports PMS, and the system resides in Bethesda, MD.

PRISM

PRISM is a contract writing system that FEMA acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation. FEMA uses an instance of PRISM, and DHS OCPO owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

An Oracle database with UNIX-based servers support PRISM, and the system resides in Datacenter 1 in Stennis, MS.

Concur Government Edition (CGE)

CGE is a third party application developed by Systems, Applications, and Products (SAP) that supports FEMA in managing travel authorizations and processing travel vouchers in compliance with government travel regulations.

Hazard Mitigation Grant Program (HMGP)

HMGP is the Mitigation module within the National Emergency Management Information System (NEMIS) Access Control System (NACS) that supports FEMA in administering grants to state and local governments to implement long-term hazard mitigation measures after a major disaster declaration. Section 404 of the Stafford Act authorizes the program and FEMA administers it. HMGP was created to reduce the loss of life and property due to natural disasters. The system resides in Mt. Weather, VA.

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. FEMA's 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 that NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. DHS components use 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. FABS is a COTS financial processing system known as Momentum, and 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 the systems of external service providers, including the USDA NFC and the GSA Concur Government Edition (CGE) electronic travel system.

An Oracle database with Microsoft Windows-based and Red Hat UNIX-based servers supports the application.

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

PRISM

PRISM is a contract writing system that FLETC acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation. FLETC uses an instance of PRISM, and the DHS OCPO owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

An Oracle database with UNIX-based servers supports PRISM, and the system resides in Datacenter 1 in Stennis, MS.

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. FLETC uses NFC and WebTA to process front-end input and certification of time and attendance entries to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application that NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. DHS components use 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. FFMS 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 that ICE's OCFO and Office of Financial Management use. FFMS also includes a desktop application that the broader ICE and USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center) use. The ICE instance of FFMS interfaces with internal ICE feeder systems and systems of external service providers, including the Department of Treasury's Bureau of the Fiscal Service and the USDA NFC.

ICE OCIO hosts and supports the ICE instance of FFMS exclusively for the ICE user community.

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

Bond Management Information System (BMIS)

BMIS is an immigration bond management database that ICE's Office of Financial Management (OFM) primarily uses. 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 Datacenter 1 in Stennis, MS, and an Oracle database and Windows servers support it.

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 problems, and geospatial information.

The application is hosted at Datacenter 1 in Stennis, MS, and an Oracle database and Windows and UNIX-based servers support it.

PRISM

PRISM is a contract writing system that ICE acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation. ICE uses an instance of PRISM, and DHS OCPO owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

An Oracle database with UNIX-based servers supports PRISM, and the system resides in Datacenter 1 in Stennis, MS.

FileOnQ (FOQ)

FOQ is ICE's official invoice tracking system. Invoices are received at the various Service Centers and are scanned/uploaded into FOQ. The invoices are then routed through different individuals for review and approval via electronic signatures.

The application is hosted at Datacenter 2 in Clarksville, VA, and an SQL Server database and Windows servers support it.

ESP

ESP is a web-based application used for Standard Form (SF)-52 processing.

ICE OCIO hosts, operates, and maintains the ESP environment, and multiple components use it. An Oracle database and Windows servers support the application, and it resides in Datacenter 1 in Stennis, MS.

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. The ICE Office of the Human Capital Officer (OHC) uses NFC and WebTA to process front-end input and certification of ICE user community time and attendance entries to facilitate payroll processing.

Management Directorate

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 records of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

ICE OCIO hosts and supports the DHS Management Directorate instance of FFMS exclusively for the DHS Management Directorate user community and, on a limited basis, for the ICE OCIO and finance center personnel providing support services for the DHS Management Directorate.

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

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. The DHS Office of Human Capital (OHC) uses NFC and WebTA to process the front-end input and certification of DHS Management Directorate user community time and attendance entries to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. DHS components use NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

National Protection and Programs Directorate (NPPD)

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.

ICE OCIO hosts and supports on behalf of NPPD the various instances of FFMS that NPPD uses exclusively for the NPPD user community and, on a limited basis, for the ICE OCIO and finance center personnel providing support services for NPPD.

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

Federal Protective Service Data System (FPSDS)

FPSDS is used to generate monthly security guard bills for other Federal agencies that use NPPD services.

The application is hosted at Datacenter 2 in Clarksville, VA, and an SQL Server database and Windows servers support it.

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. The NPPD Human Capital Office uses NFC and WebTA to process front-end input and certification of NPPD user community time and attendance entries to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and NFC Risk Management Staff developed, operate, and maintain it. DHS components use NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Science and Technology Directorate (S&T)

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.

ICE OCIO hosts and supports the S&T instance of FFMS exclusively for the S&T user community and, on a limited basis, for the ICE OCIO and finance center personnel providing support services for S&T.

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

Transportation Security Administration (TSA)

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 that CAS supports include accounts payable, accounts receivable, general and expense ledgers, and asset (including capital asset) management. CAS interfaces with internal TSA feeder systems and the systems of external service providers, including the Department of Treasury's Bureau of the Fiscal Service. The Coast Guard's OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

CAS is an Oracle Federal Financials product including an Oracle database with HP-UX and Red Hat Linux-based servers.

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) host and support CAS. It is exclusively for the TSA user community and, on a limited basis, for Coast Guard personnel performing support services for TSA.

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 that FPD perform include budgeting and funds distribution, procurement requests and simplified acquisitions, receipt of goods/services (accruals), and program element status reporting. FPD is integrated with CAS and interfaces with other internal TSA feeder systems, including the Contract Management Information System, and the systems of external service providers such as the Department of Treasury's Bureau of the Fiscal Service.

An Oracle database with Microsoft Windows, HP-UX, and Red Hat Linux-based servers supports the FPD application.

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) host and support FPD. It is exclusively for the TSA financial management and acquisitions user community and, on a limited basis, for Coast Guard personnel performing support services for TSA. The Coast Guard OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

Sunflower Asset Management System

Sunflower is a web-based application that TSA uses for property management. It comprises modules for managing inventory assets, excess assets, agreement assets, and inactive assets, and is integrated with FPD and a fixed assets module within CAS to create assets from purchase orders or receipts.

An Oracle database with Red Hat Linux-based servers supports the Sunflower application.

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) host and support Sunflower. It is exclusively for the TSA financial management and property management user community. The Coast Guard OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

MarkView

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

An Oracle database with Red Hat Linux-based servers support the MarkView application.

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) host and support MarkView. It is exclusively for the TSA financial management and procurement user community and Coast Guard Finance Center support personnel. The Coast Guard's OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

CIMS

CIMS is a contract management system used for contract creation and management. It includes milestone planning, solicitations, award, and closeout. CIMS interfaces with FPD to receive commitments and send contract procurement information. The primary users of CIMS are contracting officers and contracting specialists.

Oracle databases with Microsoft Windows servers support CIMS.

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) host and support CIMS. It is exclusively for the TSA financial management and procurement user community and Coast Guard Finance Center support personnel. The Coast Guard's OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

HRAccess

HRAccess is a collaboration of COTS and government-off-the-shelf (GOTS) information technology systems used to provide human capital services. It integrates a series of electronic and manual human capital services that were previously managed by separate systems or service providers. HRAccess streamlines human capital functions used to collect, store, and disseminate payroll, benefits, and other workforce-related information for employees and candidates.

Oracle databases with Microsoft Windows servers support HRAccess.

TSA Financial Data Warehouse (TFDW)

TFDW is a direct copy (mirror image) of the Coast Guard's CAS MIR. TFDW pulls data from MIR and is used for reporting purposes.

Oracle databases and Red Hat Linux-based servers support TFDW. 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) host and support the application. It is exclusively for the TSA financial management and procurement user community and Coast Guard Finance Center support personnel. The Coast Guard's OSC Detachment Chesapeake, in Chesapeake, VA, hosts the application.

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. TSA uses NFC and WebTA to process front-end input and certification of TSA time and attendance entries to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application that NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. DHS components use NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

United States Secret Service (USSS)

Travel Manager, Oracle Financials, Compusearch/PRISM, and Sunflower (TOPS)

TOPS is an enterprise financial management system that supports acquisition, accounting, travel, and property management functions. TOPS is a single, comprehensive, integrated financial management system that all of USSS, including field offices, use.

Oracle databases and Microsoft Windows, Solaris, and Red Hat Linux-based servers support TOPS, and it is located in Washington, DC.

WebTA

WebTA is a COTS web-based major application that USDA NFC hosts. The NFC's IT Services Division and NFC Risk Management Staff developed, operate, and maintain it. USSS uses NFC and WebTA to process front-end input and certification of USSS time and attendance entries to facilitate payroll processing.

Appendix B

FY 2016 IT Notices of Findings and Recommendations at DHS

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

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at DHS Consolidated	Security Management		X
CONS-IT-16-02	Weaknesses with DHS Treasury Information Executive Repository (DHSTIER) Baseline Configuration Policy and Procedures	Access Controls	X	
CONS-IT-16-03	Weaknesses with Procurement Request Information System Management (PRISM) Configuration Management Policy and Procedures	Configuration Management	X	

Customs and Border Protection (CBP)

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

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-09	Ineffective Design and Implementation of United States Department of Agriculture (USDA) Account Recertification Process	Access Controls	X	
CBP-IT-16-10	Lack of Annual Recertification of Automated Commercial Environment (ACE) Operating System (OS) and Database (DB) Accounts	Access Controls		X
CBP-IT-16-11	Lack of Monthly Database Vulnerability Scanning Process	Configuration Management	X	
CBP-IT-16-12	Ineffective Design of Automated Commercial Environment (ACE) Change Management Separation of Duties	Access Controls, Segregation of Duties, and Configuration Management	X	
CBP-IT-16-13	Ineffective Controls over the Mainframe Application Change Management (CM) Separation of Duties and Account Recertification Processes	Access Controls and Configuration Management	X	
CBP-IT-16-14	Ineffective Controls Over Fiscal Year (FY) 2015 IT NFR Conditions During FY 2016	Access Controls, Segregation of Duties, Configuration Management, and Contingency Planning		X
CBP-IT-16-15	Lack of Monitoring and Review of Automated Commercial Environment (ACE) Oracle Database and Database Operating System Environment Audit Logs	Access Controls	X	
CBP-IT-16-16	Lack of Access Request and Authorization Process for Automated Commercial Environment (ACE) Database Operating System Administrators	Access Controls	X	

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-17	Ineffective Controls over the Automated Commercial System (ACS) Application User Separation Process	Access Controls		X
CBP-IT-16-18	Ineffective Controls over the United States Department of Agriculture (USDA) User Account Creation Process	Access Controls	X	
CBP-IT-16-19	Ineffective Design of the Review and Protection of Human Resources Business Engine (HRBE) Operating System (OS) and CBP Directory Services (CDS) Audit Logs	Access Controls		X
CBP-IT-16-20	Lack of Systems, Applications and Products (SAP) Application Developer Account Recertification Process	Access Controls and Configuration Management	X	
CBP-IT-16-21	Ineffective Design of Automated Commercial Environment (ACE) Exadata Database Operating System Environment Patching Process	Configuration Management	X	
CBP-IT-16-22	Lack of Review of Automated Commercial Environment (ACE) Database DB2 Audit Logs and Annual Audit Log Parameters	Access Controls	X	
CBP-IT-16-23	Ineffective Design of the Human Resources Business Engine (HRBE) Application Annual Audit Log Security Configuration Review	Access Controls		X
CBP-IT-16-24	Ineffective Controls over the Automated Commercial System (ACS) User Recertification Process	Access Controls		X
CBP-IT-16-25	Lack of Access Review over Automated Commercial Environment (ACE) Users	Access Controls	X	
CBP-IT-16-26	Ineffective Design of Human Resources Business Engine (HRBE) Separation of Duties Process	Access Controls and Segregation of Duties		X
CBP-IT-16-27	Ineffective Controls over the Human Resources Business Engine (HRBE) Account Management Process	Access Controls		X

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-28	Ineffective Controls over Systems, Applications and Products (SAP) Change Management (CM) Separation of Duties	Configuration Management	X	
CBP-IT-16-29	Lack of Automated Commercial Environment (ACE) Application Developer and Production Migrator Account Recertification Process	Access Controls and Configuration Management	X	
CBP-IT-16-30	Ineffective Controls over the Human Resources Business Engine (HRBE) Application User Separation Process	Access Controls		X
CBP-IT-16-31	Ineffective Design of the Automated Commercial Environment (ACE) Red Hat Enterprise Linux (RHEL) Operating System and Oracle Database Environment Audit Logging Monitoring and Review Process	Access Controls	X	
CBP-IT-16-32	Ineffective Design of the Annual Recertification of Systems, Applications and Products (SAP) UNIX Operating System (OS) Accounts	Access Controls		X
CBP-IT-16-33	Ineffective Design of the CBP Cloud Computing Environment (C3E) and CBP Directory Services (CDS) Account Recertification Processes	Access Controls		X
CBP-IT-16-34	Ineffective Controls over Systems, Applications, Products (SAP) UNIX Operating System (OS) Identification and Authentication Processes	Access Controls		X
CBP-IT-16-35	Weaknesses Identified during the Vulnerability Assessment of the Authorized Desktop Build (ADB), CBP Directory Services (CDS), Human Resource Business Engine (HRBE), and Systems, Applications and Products (SAP) Environment	Configuration Management		X
CBP-IT-16-36	Ineffective Controls over the Automated Commercial System (ACS) User Account Creation Process	Access Controls		X

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-16-37	(Withdrawn)	NA	NA	NA
CBP-IT-16-38	Ineffective Controls over the Systems, Applications and Products (SAP) Application Access Separation Process	Access Controls		X
CBP-IT-16-39	Ineffective Controls over the Human Resources Business Engine (HRBE) Weekly Backups	Contingency Planning	X	
CBP-IT-16-40	Lack of Functionality in the Automated Commercial System (ACS)	Business Process Application Controls		X

United States Coast Guard (USCG)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-16-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Entity Level		X
CG-IT-16-02	Ineffective Controls over NESSS Application Account Management	Access Controls	X	
CG-IT-16-03	Weakness in Direct Access Database Password Configurations Associated with the PeopleSoft Application/System Accounts	Access Controls		X
CG-IT-16-04	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCG	Security Management		X
CG-IT-16-05	Weakness in Review of Database Audit Log Review for NESSS, NPFC, and SAM	Access Controls	X	
CG-IT-16-06	Weakness in SAM Database Password Configurations and Shared Account Usage	Access Controls	X	
CG-IT-16-07	Weakness in Developer Access to Production for NESSS	Access Controls and Configuration Management	X	
CG-IT-16-08	Weakness in Developer Access to Production for NPFC-CIMS	Access Controls and Configuration Management	X	
CG-IT-16-09	Ineffective Controls over Direct Access Account Maintenance	Access Controls	X	
CG-IT-16-10	Weakness in EmpowHR Privileged Accounts	Access Controls	X	
CG-IT-16-11	Ineffective Controls over NESSS Operating System User Recertification	Access Controls		X
CG-IT-16-12	Ineffective Design over NESSS Database User Recertification	Access Controls		X

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-16-13	Ineffective Design over NPFC-CIMS Database User Recertification	Access Controls		X
CG-IT-16-14	Ineffective Design over SAM Database User Recertification	Access Controls	X	
CG-IT-16-15	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant OSC, ALC and FINCEN Hosted Environments	Access Controls and Configuration Management		X
CG-IT-16-16	Ineffective Controls over Periodic Review of Access Authorization for ALMIS	Access Controls	X	
CG-IT-16-17	Lack of Controls over Segregation of Duties within the Workflow Imaging Network System (WINS)	Segregation of Duties		X
CG-IT-16-18	Ineffective Controls over the Open Obligation Validation Application (OOVA) User Account Creation Process	Access Controls	X	

United States Citizenship and Immigration Services (USCIS)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-16-02	Lack of Configuration Management Plan for the Electronic Immigration System (ELIS2)	Configuration Management	X	
CIS-IT-16-03	Unsigned ESP User Access Forms	Access Controls	X	
CIS-IT-16-04	Weakness in ESP Quarterly Account Recertification	Access Controls	X	
CIS-IT-16-05	Inadequate Audit Logging and Account Management and Recertification for the Electronic Immigration System (ELIS2) Environment	Access Controls		X
CIS-IT-16-06	Lack of WebTA User Access Forms	Access Controls		X
CIS-IT-16-07	FFMS Deficiencies at ICE that Impact USCIS	Access Controls	X	

Federal Emergency Management Agency (FEMA)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-16-01	Non-Compliance with Alternate Processing Site Requirements for Key Financial Systems	Contingency Planning		X
FEMA-IT-16-02	Insufficient Audit Log Controls for Key Financial Systems	Access Controls		X
FEMA-IT-16-03	Network Access Control Systems (NACS) Account Management Weakness	Access Controls		X
FEMA-IT-16-04	Non-Compliance with Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls		X
FEMA-IT-16-05	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-16-06	Weaknesses within Web Time and Attendance (WebTA) Account Management Policies and Procedures	Access Controls		X
FEMA-IT-16-07	Inconsistent Implementation of EmpowHR Account Management Controls	Access Controls		X
FEMA-IT-16-08	Weaknesses with CGE Account Management Controls	Access Controls	X	
FEMA-IT-16-09	Non-Compliance with DHS Policy for Elevated Privileged (EP) Server Access	Access Controls and Configuration Management	X	
FEMA-IT-16-10	Inconsistent Authorization of Privileged Access for Systems Managed by OCIO IT Operations	Access Controls	X	
FEMA-IT-16-11	Weaknesses with Monitoring and Enforcing Role-Based Training for Individuals with Significant Information Security Responsibilities	Security Management		X

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-16-12	Non-Compliant Plan of Action and Milestone (POA&M) Reporting for Key Financial Systems	Access Controls		X
FEMA-IT-16-13	Weaknesses with Implementation of Separated User Access Controls for Key Financial Systems	Access Controls	X	
FEMA-IT-16-14	Weaknesses with PRISM Account Management Policy and Procedures	Access Controls	X	
FEMA-IT-16-15	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted at the Mount Weather Emergency Operations Center (MWEOC)	Access Controls and Configuration Management		X
FEMA-IT-16-16	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted by NFIP ITS	Access Controls and Configuration Management	X	

Federal Law Enforcement Training Center (FLETC)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-16-01	Non-Compliance with Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls		X
FLETC-IT-16-02	Insufficient Audit Log Controls for Key Financial Systems	Access Controls	X	
FLETC-IT-16-03	Excessive Non-Unique Database Access Privileges	Access Controls	X	
FLETC-IT-16-04	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted at DC1	Configuration Management		X

United States Immigration and Customs Enforcement (ICE)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-IT-16-02	Non-Compliance with DHS Policies Related to Oracle Database Password Configurations for the Federal Financial Management System (FFMS)	Access Controls	X	
ICE-IT-16-03	Insufficient Audit Log Controls for the Real Property Management System (RPMS)	Access Controls	X	
ICE-IT-16-04	Insufficient Audit Log Controls for the Bonds Information Management System (BMIS)	Access Controls	X	
ICE-IT-16-05	Non-Compliance with DHS Policies Related to Oracle Database Password Control Deficiencies for the Real Property Management System (RPMS)	Access Controls	X	
ICE-IT-16-06	Non-Compliance with DHS Policies Related to Oracle Database Password Control Deficiencies for the Bonds Information Management System (BMIS)	Access Controls	X	
ICE-IT-16-07	Inconsistent Account Management Controls of Privileged Access for Web Time and Attendance (WebTA)	Access Controls	X	
ICE-IT-16-08	Security Awareness Issues Identified during Social Engineering Testing at ICE	Security Management		X
ICE-IT-16-09	Weakness with Bonds Management Information System (BMIS) Privileged User Semi-Annual Recertification Process	Access Controls	X	

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-16-10	Weakness with Real Property Management System (RPMS) Privileged User Semi-Annual Recertification Process	Access Controls	X	
ICE-IT-16-11	Weakness in FileOnQ (FOQ) Configuration Management Controls	Configuration Management	X	
ICE-IT-16-12	Non-Compliance Delegation of Authority for Federal Financial Management System (FFMS), Bonds Management Information System (BMIS) and FileOnQ (FOQ)	Security Management	X	
ICE-IT-16-13	Lack of FFMS Account Management Policies and Procedures for Privileged User Access to the Operating System and Database	Access Controls	X	
ICE-IT-16-14	Weakness with FFMS Privileged User Semi-Annual Recertification Process	Access Controls	X	
ICE-IT-16-15	Insufficient Audit Log Controls for the FFMS Operating System	Access Controls	X	
ICE-IT-16-16	Deficiency in PRISM User Account Authorization Process	Access Controls	X	
ICE-IT-16-17	Deficiency in ICE FFMS User Account Authorization Process	Access Controls		X
ICE-IT-16-18	Weakness with Implementation of Separated User Access Control for FFMS	Access Controls	X	
ICE-IT-16-19	Deficiency in ICE WebTA User Account Authorization Process	Access Controls		X
ICE-IT-16-20	Weakness with ESP Account Management Controls	Access Controls	X	
ICE-IT-16-21	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted by ICE HQ, DC1 and DC2	Access Controls and Configuration Management	X	
ICE-IT-16-22	Weakness in FOQ Account Management Controls	Access Controls	X	

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-16-23	Incomplete Documentation for FFMS Configuration Management Controls	Configuration Management	X	
ICE-IT-16-24	Weakness with PRISM Annual User Recertification Process	Access Controls	X	

Management Directorate

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
MGT -IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at Management Directorate	Security Management		X
MGT -IT-16-02	Deficiency in Web Time and Attendance (WebTA) User Account Authorization Process	Access Controls		X
MGT -IT-16-03	Inability to Generate a Complete and Accurate Listing of Separated Contractors	Access Controls		X
MGT -IT-16-04	Deficiency in EmpowHR User Account Authorization Process	Access Controls		X
MGT -IT-16-05	FFMS Deficiencies at ICE that Impact Management Operations	Access Controls and Configuration Management	X	

National Protection and Programs Directorate (NPPD)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
NPPD-IT-16-01	Weakness with WebTA Account Management Controls	Access Controls	X	
NPPD-IT-16-02	FPSDS Account Management Weakness	Access Controls	X	
NPPD-IT-16-03	Inability to Generate a Complete and Accurate Listing of Separated Contractors	Access Controls		X
NPPD-IT-16-04	Weakness with EmpowHR Account Management Controls	Access Controls	X	
NPPD-IT-16-05	FFMS Deficiencies at ICE that Impact NPPD Operations	Access Controls and Configuration Management	X	

Science and Technology Directorate (S&T)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ST-IT-16-01	FFMS Deficiencies at ICE that Impact S&T Operations	Access Controls and Configuration Management	X	

Transportation Security Administration (TSA)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-16-01	Security Awareness Issues Identified During After-Hours Physical Security Testing at TSA	Security Management		X
TSA-IT-16-02	Weakness in HRAccess Database Password Configurations	Access Controls	X	
TSA-IT-16-03	Lack of Periodic Reviews of Access Authorization	Access Controls	X	
TSA-IT-16-04	Ineffective Controls over Removing Access for Inactive and Separated User Accounts	Access Controls	X	
TSA-IT-16-05	Weakness in Management Approving Database Accounts	Access Controls	X	
TSA-IT-16-06	Ineffective Controls over Removing and Disabling Access for Separated Employees in WebTA	Access Controls	X	

United States Secret Service (USSS)

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
USSS-IT-16-01	Security Awareness Issues Identified During After-Hours Physical Security Testing at USSS Headquarters	Security Management		X
USSS-IT-16-02	Ineffective Profile Settings and Controls for TOPS Database Security	Access Controls	X	
USSS-IT-16-03	Ineffective Controls Over TOPS Database and Operating System Security Audit Log Review	Access Controls	X	
USSS-IT-16-04	Ineffective Design Over TOPS Operating System Administrator Account Recertification	Access Controls	X	
USSS-IT-16-05	Inadequate Documentation for TOPS Application and Database Privileged User Account Management	Access Controls	X	
USSS-IT-16-06	Inadequate Controls over USSS' Instance of Web Time and Attendance (WebTA)	Access Controls		X
USSS-IT-16-07	Weakness in TOPS Segregation of Duties	Segregation of Duties	X	
USSS-IT-16-08	Security Awareness Issues Identified during Social Engineering Testing at USSS	Security Management	X	
USSS-IT-16-09	Weakness in TOPS Application Authentication	Access Controls	X	
USSS-IT-16-10	Ineffective Design Over TOPS Database Administrator Account Recertification	Access Controls	X	
USSS-IT-16-11	Inadequate Documentation for TOPS Operating System Privileged User Account Management	Access Controls	X	

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
USSS-IT-16-12	Inadequate Design Over TOPS Application User Account Recertification	Access Controls	X	
USSS-IT-16-13	Ineffective Controls Over Timely Removal of Accounts for Terminated Individuals within TOPS	Access Controls	X	
USSS-IT-16-14	Security Management and Configuration Management Controls – Vulnerability Assessment	Configuration Management	X	

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
Acting 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