OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the FY 2014 Department of Homeland Security Financial Statement Audit

Homeland Security

May 19, 2015

OIG-15-93

DHS OIG HIGHLIGHTS

Information Technology Management Letter for the FY 2014 Department of Homeland Security Financial Statement Audit

May 19, 2015

Why We Did This

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

What We Recommend

We recommend the Chief Information Officer and Chief Financial Officer work with components to make improvements to DHS' financial management systems and associated information technology security program.

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

What We Found

We contracted with the independent public accounting firm KPMG LLP (KPMG) to perform the audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS) for the year ended September 30, 2014. KPMG evaluated selected general information technology controls, and information technology (IT) entity-level controls, and business process application controls at DHS' components. KPMG noted that the DHS Components made progress in the remediation of certain IT deficiencies we reported in FY 2013, approximately 35 percent of the prior year IT deficiencies.

KPMG continued to identify deficiencies related to access controls, segregation of duties controls, and configuration management controls of DHS' core financial system. KPMG noted that limitations in DHS Components' financial systems' functionality are inhibiting the Department's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data.

The findings collectively limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. The deficiencies at Customs and Border Protection, the U.S. Coast Guard, and the Federal Emergency Management Agency adversely impacted the internal controls over DHS' financial reporting and its operation and collectively represent a material weakness reported in the FY 2014 DHS Agency Financial Report.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC

May 19, 2015

TO: Luke McCormack
Chief Information Officer

Chip Fulghum
Chief Financial Officer

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

SUBJECT: *Information Technology Management Letter for the FY 2014 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2014 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 2014 Financial Statements and Internal Control over Financial Reporting,* dated November 14, 2014, which was included in the FY 2014 DHS Agency Financial Report.

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

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

Attachment

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

December 8, 2014

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

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department), as of and for the year ended September 30, 2014, 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. 14-02, *Audit Requirements for Federal Financial Statements*, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the consolidated financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

During our audit, we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies. During our audit we noted certain matters involving financial reporting internal controls (comments not related to 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 OIG and the DHS Chief Financial Officer.

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

Additionally, at the request of the DHS Office of Inspector General (OIG), we performed certain procedures to assess the adequacy of non-technical measures to secure sensitive IT and financial information and assets from unauthorized access or disclosure. We noted instances where DHS Component personnel did not consistently apply the principles communicated in ongoing security awareness training related to these measures. These matters are described in the *Observations Related to Non-Technical Information Security Awareness Weaknesses* section of this letter.

We have provided a description of key DHS and Component financial systems and IT infrastructure within the scope of the FY 2014 DHS financial statement audit in Appendix A, and a listing of each IT NFR 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 to you.

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

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

DHS' response to the deficiencies identified in our audit is described in page 13 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, 2014

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, 2014 (referred to herein as the "fiscal year (FY) 2014 financial statements"). In connection with our audit of the FY 2014 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs), IT entity-level controls (ELCs), and IT application controls at DHS components to assist in planning and performing our audit engagement. At the request of the DHS Office of Inspector General (OIG), we also performed additional information security testing procedures to assess certain non-technical areas related to the protection of sensitive IT and financial information and assets.

Scope and Approach

General Information Technology Controls and IT Entity-Level Controls

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

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

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

While each of these five FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs and IT ELCs for evaluation based on their relationship to the ongoing effectiveness of process-level automated controls or manual controls with one or more automated

components. This includes those controls which depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2014 GITC and IT ELC procedures at each DHS component did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

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

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

Financial System Functionality

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

Non-Technical Information Security Testing

To complement our IT controls test work, we conducted limited after-hours physical security testing and social engineering at selected 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 2014 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 2014 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2014 assessment of GITCs, IT ELCs, and IT application controls, we noted that the DHS components made progress in the remediation of certain IT findings we reported in FY 2013. We closed approximately 35 percent of our prior year IT findings. However, new findings were noted in most DHS components in FY 2014, many of which were either (1) related to controls that were effective in prior years, or (2) control deficiencies noted over new systems that were similar to deficiencies previously reported.

In FY 2014, we issued 103 total findings, of which approximately 48 percent were repeated from the prior year. Approximately 57 percent of our repeat findings were for IT deficiencies that management represented were corrected during FY 2014. The new findings in FY 2014, noted at nearly all DHS components, resulted from additional IT systems and business processes within the scope of our audit this year and from control deficiencies identified in areas that were effective in previous years.

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

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

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we noted that limitations in DHS components' financial systems' functionality may be inhibiting the Department's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data. At many components, key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Many key DHS financial systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and Office of Management and Budget (OMB) Circular Number A-123 Appendix D, *Compliance with FFMIA.*

The conditions supporting our findings collectively limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, certain of these deficiencies at Customs and Border Protection (CBP), the U.S. Coast Guard (Coast Guard), and the Federal Emergency Management Agency (FEMA) 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. Certain of the IT findings issued at CBP, Coast Guard, and FEMA were combined into one material weakness regarding *IT*

Controls and Financial System Functionality for the FY 2014 DHS consolidated financial statements audit.

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

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

FINDINGS AND RECOMMENDATIONS

Findings

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

Deficiencies Related to IT Controls

Security Management

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

- Required security authorization activities and artifacts supporting key financial systems were not always completed and documented timely, accurately, or otherwise in accordance with DHS requirements.

- At one component, an interconnection security agreement (ISA) had expired and was not renewed in a timely manner.

Access Controls

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

- Initial authorization and periodic recertification of application, database, and operating system user, service, and generic accounts (including emergency and temporary access) were inadequate, inconsistent, or in violation of the principles of least privilege and segregation of duties.

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

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

- 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.

- Physical access to the interior rooms of facilities hosting key DHS financial systems was not consistently recertified.

Configuration Management

- Security patch management and configuration deficiencies were identified during vulnerability assessments of servers, system software, and databases supporting key financial applications and general support systems.

- Vulnerability management activities, including internal scans of financial applications and system software and implementation of vendor-recommended patches to address known vulnerabilities, were not consistently performed.

- Monitoring controls to ensure the completeness and integrity of records regarding changes to key financial systems were not always implemented.

- At one component, audit procedures over certain controls and application functionality were performed in one financial system's test environment. However, component personnel were unable to provide evidence in a timely manner that the test environment appropriately mirrored the production environment.

- Configuration changes to financial systems were not consistently tested before deployment to production.

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

Segregation of Duties

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

Contingency Planning

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

IT Application Controls

- One component was unable to identify an appropriate point of contact to demonstrate application control procedures.

Deficiencies Related to Financial Systems Functionality

In addition to the IT control deficiencies noted above, we identified many instances across all DHS components where financial system functionality limitations were inhibiting DHS' 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 was outdated and no longer supported by the respective vendors. This resulted in unmitigated vulnerabilities that exposed underlying data to potential unauthorized and undetected access and exploitation.

- General IT controls and financial process areas were implemented or supported by highly-manual processes, outdated or decentralized systems and records management processes, or utilities with limited automated capabilities. These limitations introduced a higher 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 provide readily auditable transaction populations without substantial manual intervention and additional supporting information.

In addition to these general areas, system limitations contributed to deficiencies in multiple financial process areas across the DHS components. System configurations and posting logic deficiencies limited the effectiveness of controls to properly calculate the value of certain transactions, require authorized officials' approvals for certain transactions, and identify funding variances, as well as to enforce requirements for required approvals, prevent or detect and correct excessive refund claims, implement general ledger accounts in compliance with FFMIA, or properly and accurately record opening balances. Effective monitoring controls, including tracking and reconciliation of intragovernmental and grant program-related transactions were also impaired by system limitations. In some cases, components implemented manual processes for entry, recalculation, or adjustment of data to compensate for these limitations, but these manual processes were prone to error and increased the risk that financial data and transactions were improperly posted to the respective systems.

Cause

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

Effect

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

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

Recommendation

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

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY AWARENESS

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

Social Engineering

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

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

Component	Number of Calls Attempted	Number of Individuals Reached	Number of Exceptions Noted
CBP	60	51	1
USCG	51	29	5
CIS	45	13	1
CONS	45	8	0
FEMA	45	14	2
ICE	45	17	0
TSA	55	24	2
USSS	40	9	1
MGT	45	21	3

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

After-Hours Physical Security Walkthroughs

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

We performed procedures to determine whether DHS component personnel consistently exercised responsibilities related to safeguarding sensitive materials as defined in these policies. Specifically, we performed escorted walkthroughs of workspaces – including cubicles, offices, shared workspaces, and/or common areas (e.g., areas where printers were hosted) – at component facilities that processed, maintained, and/or had access to financial data during FY 2014. We inspected workspaces to identify instances where materials designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from the component, DHS OIG, and DHS OCIO.

At each component where after-hours physical security walkthroughs were performed, we noted instances where material – including but not limited to system passwords, information marked "FOUO" or otherwise meeting the criteria established by DHS MD 11042.1, documents containing sensitive PII, and government-issued laptops, mobile devices, or storage media – was left unattended and unsecured after business hours in violation of DHS policy.

Component	Number of Workspaces Inspected	Number of Workspaces with Exceptions Noted
CBP	120	26
USCG	270	84
CIS	45	13
CONS	53	5
FEMA	220	61
ICE	79	22
TSA	72	38
USSS	40	20
MGT	28	11

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

MANAGEMENT RESPONSE

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

Appendix A

Description of Key DHS Financial Systems and IT Infrastructure Within the Scope of the FY 2014 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 2014 financial statement audit.

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

DHS Treasury Information Executive Repository (DHSTIER)

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

Customs and Border Protection (CBP)

Automated Commercial Environment (ACE)

ACE is a web-based major application that CBP uses to track, control, and process commercial goods and conveyances entering the United States for the purpose of collecting import duties, fees, and taxes owed to the Federal government. It includes functionality to calculate monthly statements for importers and perform sampling and audits of import/entry transactions. It was developed to replace the Automated Commercial System (ACS).

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

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

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

Automated Commercial System (ACS)

ACS is a mainframe-based major application comprised of subsystems CBP uses to track, control, and process commercial goods and conveyances entering the United States territory for the purpose of collecting import duties, fees, and taxes owed to the Federal government. It includes functionality to calculate monthly statements for importers and perform sampling and audits of import/entry transactions.

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

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

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

Systems, Applications, and Products (SAP)

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

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

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

Computerized Aircraft Reporting and Material Control System (CARMAC)

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

CARMAC is developed and maintained by the CBP Office of Air and Marine and the CBP Office of Information and Technology, and hosted and supported by CSC contractor personnel exclusively for internal use by the CBP Office of Air Marine and Defense Support Services user community.

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

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

The AD and ADB General Support Systems environment is maintained by CBP EDMED, and hosted and supported by the CBP Office of Information Technology exclusively for internal use by the CBP user community.

United States Coast Guard

Core Accounting System (CAS)

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

CAS is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard user community.

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 ledger management, budgeting and funds distribution, procurement requests and simplified acquisitions, receipt of goods/services (accruals), and program element status reporting. It is integrated with CAS and contains interfaces with the DHS Treasury Information Executive Repository, other internal Coast Guard feeder systems (including the Contract Management Information System), and external service providers (including the Department of Treasury's Bureau of the Fiscal Service).

FPD is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard financial management and acquisitions user community.

Direct Access

Direct Access is a web-based major application and the system of record for all payroll events for the Coast Guard. Direct Access supports "self-service" capabilities for end-user updates and corrections to personal information, including beneficiary designations, and is used by the Coast Guard Pay & Personnel Center (PPC) to process payroll events and perform personnel actions, such as pay scales updates. It contains interfaces with other internal Coast Guard feeder systems, including the Joint Uniform Military Pay System, and external service providers such as the United States Public Health Service and the Department of Veterans Affairs. Global Pay, a module within Direct Access, provides retiree and annuitant support services.

Direct Access is developed, maintained, and hosted by Addx Corporation. It is supported by Coast Guard OCIO for internal use by the Coast Guard user community and for external public (authenticated) access by Coast Guard retirees.

Joint Uniform Military Pay System (JUMPS)

JUMPS is a mainframe-based major application used for computations of all information needed to pay Active Duty and Reservist military members. It contains interfaces with other internal Coast Guard feeder systems, including Direct Access.

JUMPS is developed, maintained, and hosted by the Coast Guard Operations Systems Center (a component of the Office of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology), and supported by Coast Guard PPC exclusively for internal use by the Coast Guard user community.

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.

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

Aviation Logistics Management Information System (ALMIS)

ALMIS is a hybrid web-based and client-server major application that provides Coast Guard aviation logistics management support in the areas of operations, configuration management, maintenance, supply, procurement, financial management, and business intelligence. It integrates the forecasting capability of the Aviation Computerized Maintenance Systems (ACMS) subsystem with the inventory management

and fiscal accounting functionality of the Aviation Maintenance Management System (AMMIS) subsystem to improve inventory purchase/repair decisions and provide total asset visibility.

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

Immigration and Customs Enforcement (ICE) and 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 ICE and USCIS. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable issued. The system supports all internal and external financial reporting requirements.

FFMS includes a back-office component used by the ICE and USCIS OCFO, the ICE Office of Financial Management, and the USCIS Financial Management Division. FFMS also includes a desktop application used by the broader ICE and USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center). The ICE instance of FFMS contains interfaces with internal ICE feeder systems and external service providers, including the Department of Treasury's Bureau of the Fiscal Service and the USDA's National Finance Center (NFC). The USCIS instance of FFMS contains no known internal or external interfaces.

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

Federal Emergency Management Agency (FEMA)

Web Integrated Financial Management Information System (WebIFMIS)

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

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

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

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 (OCFO) component provides FEMA staff with the ability to view SF 425 submissions, examine grantee payment history reports, and add or remove holds on grantee payments.

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

Non-Disaster Grant Management System (NDGrants)

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

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

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

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 needed to protect the public and emergency personnel from fire and related hazards.

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

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

Emergency Management Mission Integrated Environment (EMMIE)

EMMIE is a web-based major application used by FEMA program offices and user communities directly involved in the grant lifecycles associated with the Public Assistance grant program. These include Fire Management Assistance grants, to provide assistance to State, Tribal and local governments, and certain types of private nonprofit organizations so that communities can quickly respond to and recover from major disasters or emergencies declared by the President.

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

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

Emergency Support (ES)

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

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

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

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

Transaction Recording and Reporting Processing (TRRP)

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

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

Payment Management System (PMS)

The PMS, commonly referred to as Smartlink, is a web-based major application hosted, developed, operated, and maintained by the HHS National Institutes of Health (NIH) Center for Information Technology (CIT) Information Systems Branch (ISB). The FEMA OCFO FEMA 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.

Web Time and Attendance (WebTA)

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

Federal Law Enforcement Training Center (FLETC), the Office of Intelligence & Analysis (I&A) and the Office of Operations Coordination and Planning (OPS)

Financial Accounting and Budgeting System (FABS)

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

Under the terms of a Memorandum of Understanding, FLETC provides financial management services to I&A and OPS through a separately-hosted instance of the FABS environment, which was developed to mirror the FLETC FABS environment.

FABS is hosted and supported by the FLETC IT Infrastructure Branch and the FLETC OCFO Finance Division on behalf of I&A and OPS and under the terms of the Memorandum of Understanding between the two Components. FABS is exclusively for internal use by the FLETC, I&A, and OPS user communities.

Transportation Security Administration (TSA)

Core Accounting System (CAS)

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

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

Finance Procurement Desktop (FPD)

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

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

Sunflower Asset Management System

Sunflower is a web-based, COTS major application used by TSA for property management. It is comprised of modules including the management of inventory assets, excess assets, agreement assets, and

inactive assets, and is integrated with FPD and the fixed assets module within CAS to create assets from purchase orders or receipts.

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

MarkView

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

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

Electronic Time Attendance and Scheduling (eTAS)

eTAS is a web-based major application that provides an automated and standardized labor management solution for scheduling, recording, and reporting TSA Transportation Security Officer (TSO) employee work and leave hours via interface to WebTA, and subsequently to TSA's payroll provider, the USDA NFC.

eTAS is hosted at the DHS OCIO Enterprise Data Center (DC-2) and is supported by DC-2 contract technical support – including CSC, Inc., operating under the TSA Information Technology Infrastructure Program (ITIP) contract, and International Business Machines, Inc., operating under the Operational Application Support and Information Services (OASIS) contract – on behalf of the TSA Office of Human Capital. eTAS is exclusively for internal use by the TSA TSO user community.

Appendix B

FY 2014 IT Notices of Findings and Recommendations at DHS

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

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-14-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at OFM	Security Management		X
CONS-IT-14-02	Weaknesses Identified during the Vulnerability Assessment on DHSTIER	Configuration Management	X	
CONS-IT-14-03	Lack of Documented Agreement between DHS and the National Aeronautics and Space Administration (NASA) for Assignment of Control Responsibility for Physical Access Controls over the DHSTIER System Environment	Access Controls		X

Customs and Border Protection (CBP)

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

CBP-IT-14-12	Lack of ACE Linux OS Inactivity Parameters	Access Controls	X	
CBP-IT-14-13	Separated Personnel on the ACS Application User Listing	Access Controls	X	
CBP-IT-14-14	Configuration Management and Separation of Duties Weaknesses within the ACE	Configuration Management	X	
CBP-IT-14-15	Lack of Monthly Vulnerability Scans Performed over the ACE	Configuration Management	X	
CBP-IT-14-16	Lack of Review and Protection of CARMAC Application and Mainframe Audit Logs	Access Controls	X	
CBP-IT-14-17	Weaknesses in Creating New CARMAC TSO Mainframe Accounts	Access Controls	X	
CBP-IT-14-18	Lack of Patching Performed over the CARMAC Mainframe	Configuration Management	X	
CBP-IT-14-19	Separated Personnel on the ADB AD Network User Listing	Access Controls		X
CBP-IT-14-20	Failure to Identify Knowledgeable Personnel for Discussion Regarding Accelerated Payment Privileges	Business Process Controls	X	
CBP-IT-14-21	Inappropriately Configured Audit Log Parameters for SAP UNIX OS	Access Controls	X	
CBP-IT-14-22	Lack of Annual Recertification of CARMAC Application and Mainframe Generic, Non-human accounts; Deficiencies in CARMAC Application and Mainframe Generic, Non-human Accounts Retaining Unnecessary Access	Access Controls	X	
CBP-IT-14-23	Weakness in Testing ACS Configuration Management Changes Prior to Implementation into the Production Environment	Configuration Management	X	
CBP-IT-14-24	Separated Personnel on the CARMAC Application User Listing	Access Controls	X	
CBP-IT-14-25	Lack of Comparable ACS Test and Production Environments	Business Process Controls/ Configuration Management	X	
CBP-IT-14-26	Inappropriately Configured Inactivity Parameters for the CARMAC	Access Controls	X	

	Application and Mainframe			
CBP-IT-14-27	Lack of ACE Oracle DB Inactivity Parameters	Access Controls	X	
CBP-IT-14-28	ACE Configuration Baseline Weaknesses	Configuration Management	X	
CBP-IT-14-29	Lack of Functionality in the ACS	Business Process Controls		X
CBP-IT-14-30	Deficiencies in Renewal of ISAs	Security Management	X	
CBP-IT-14-31	Deficiencies in Security Awareness and Role-based Training Programs	Security Management/ Access Controls	X	

United States Coast Guard (USCG)

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-14-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Access Controls		X
CG-IT-14-02	JUMPS audit log review	Access Controls	X	
CG-IT-14-03	Inappropriate access to JUMPS Production Library Datasets	Access Controls	X	
CG-IT-14-04	Weakness in Direct Access Annual User Recertification	Access Controls		X
CG-IT-14-05	AMMIS System Administrator Account Lockouts for Invalid Login Attempts	Access Controls	X	
CG-IT-14-06	Security Awareness Issues Identified during Social Engineering Testing at Coast Guard Headquarters, SFLC/Coast Guard Yard; FINCEN	Security Management		X
CG-IT-14-07	Review of Direct Access Security Logs	Access Controls		X
CG-IT-14-08	Direct Access Database Profile Security Configurations	Access Controls	X	
CG-IT-14-09	Security Awareness Issues Identified during After-Hours Physical Security Testing at Coast Guard	Security Management		X
CG-IT-14-10	NESSS Database Profile Security Configurations	Access Controls	X	
CG-IT-14-11	NESSS System User Access	Access Controls	X	
CG-IT-14-12	FPD Audit Log Reviews	Access Controls	X	
CG-IT-14-13	Weakness in JUMPS Annual User Recertification	Access Controls		X
CG-IT-14-14	Security Management and Configuration Management Controls - Vulnerability Assessment	Configuration Management		X

United States Citizenship and Immigration Services (USCIS)

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-14-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-14-02	Security Awareness Issues Identified during Social Engineering Testing at USCIS	Security Management		X
CIS-IT-14-03	Deficiency in USCIS FFMS User Account Modification Process	Access Controls	X	
CIS-IT-14-04	Deficiency in USCIS FFMS User Account Termination Process and Attrition Process	Access Controls		X
CIS-IT-14-05	FFMS Vulnerability Weaknesses Impact USCIS Operations	Configuration Management		X

Federal Emergency Management Agency (FEMA)

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-14-01	Security Awareness Issues Identified during Social Engineering Testing at FEMA	Security Management	X	
FEMA-IT-14-02	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-14-03	Non-Compliant Security Authorization Package for PARS	Security Management	X	
FEMA-IT-14-04	Non-Compliance with Alternate Processing Site Requirements for Key Financial Systems	Contingency Planning		X
FEMA-IT-14-05	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the EMMIE, NDGrants, ES, and AFG Systems	Configuration Management		X
FEMA-IT-14-06	Non-Compliant Security Authorization Package for NDGrants	Security Management		X
FEMA-IT-14-07	Non-Compliant Security Authorization Package for WebIFMIS	Security Management		X
FEMA-IT-14-08	Non-Compliant Security Authorization Package for ES	Security Management	X	
FEMA-IT-14-09	Non-Compliant Security Authorization Package for AFG	Security Management	X	
FEMA-IT-14-10	Lack of WebTA Account Management Policies and Procedures	Access Controls	X	
FEMA-IT-14-11	Weaknesses Identified during the Vulnerability Assessment on WebIFMIS	Configuration Management		X
FEMA-IT-14-12	Weaknesses Identified during the Vulnerability Assessment on the NFIP ITS	Configuration Management		X
FEMA-IT-14-13	Weaknesses Identified during the Vulnerability Assessment on	Configuration Management		X

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
	Financially Significant Segments of the FEN and End-User Computing Environment			
FEMA-IT-14-14	Weaknesses Identified during the Vulnerability Assessment on EMMIE	Configuration Management		X
FEMA-IT-14-15	Weaknesses Identified during the Vulnerability Assessment on the NDGrants and AFG Systems	Configuration Management		X
FEMA-IT-14-16	Insufficient Audit Log Controls for Key Financial Systems	Access Controls	X	
FEMA-IT-14-17	Incomplete Implementation of Role-Based Training for Individuals with Significant Information Security Responsibilities	Security Management		X
FEMA-IT-14-18	Inconsistent Delegation of Authority and Authorization of Database Elevated Privileges and Developer Access for Key Financial Systems	Access Controls		X
FEMA-IT-14-19	Incomplete Account Management Documentation for ES	Access Controls		X
FEMA-IT-14-20	Inconsistent Authorization of EMMIE Application User Access	Access Controls	X	
FEMA-IT-14-21	Incomplete Account Management Documentation for the AFG Application	Access Controls	X	
FEMA-IT-14-22	Non-Compliance with DHS and FEMA Password Requirements for Legacy Accounts on the Oracle Databases Supporting Certain Financial Applications	Access Controls		X
FEMA-IT-14-23	Non-Compliance with DHS Secure Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls	X	
FEMA-IT-14-24	Incomplete Documentation of WebIFMIS Application Functions	Segregation of Duties		X
FEMA-IT-14-25	Inconsistent Implementation of WebIFMIS and PARS Audit Log Controls	Access Controls		X

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-14-26	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the WebIFMIS and PARS Production Environments	Configuration Management		X
FEMA-IT-14-27	Lack of Configuration Management Plan for the PARS Application Production Environment	Configuration Management	X	
FEMA-IT-14-28	Lack of Smartlink Account Management Policies and Procedures	Access Controls	X	

**Federal Law Enforcement Training Center (FLETC), the
Office of Intelligence & Analysis (I&A), and the Office of Operations Coordination and Planning (OPS)**

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-14-01	FLETC Contractor Separation Listing	Access Controls		X
IAOPS-IT-14-01	Contractor Separation Listing	Access Controls		X
IAOPS-IT-14-02	Separation Process	Access Controls		X

United States Immigration and Customs Enforcement (ICE)

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-14-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-IT-14-02	Deficiency in ICE FFMS User Account Authorization Process	Access Controls		X
ICE-IT-14-03	Deficiency in ICE FFMS User Separation Process	Access Controls		X
ICE-IT-14-04	Deficiency in the FFMS Temporary User Access Process	Access Controls	X	
ICE-IT-14-05	FFMS Mainframe Production databases were installed and configured without baseline security configurations	Configuration Management		X
ICE-IT-14-06	ICE workstations were installed with miss-configuration and missing patches	Configuration Management	X	

Management Directorate (MGT)

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
MGT-IT-14-01	Security Awareness Issues Identified during Social Engineering Testing at MGT	Security Management	X	
MGT-IT-14-02	Security Awareness Issues Identified during After-Hours Physical Security Testing at MGT	Security Management	X	

Transportation Security Administration (TSA)

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-14-01	Physical Security and Security Awareness Issues Identified During After Hours Testing at TSA	Security Management		X
TSA-IT-14-02	Security Awareness Issues Identified During Social Engineering Testing at TSA Headquarters	Security Management		X
TSA-IT-14-03	eTAS user account management	Access Controls		X
TSA-IT-14-04	Weakness in eTAS review of audit logs	Access Controls		X
TSA-IT-14-05	eTAS Database Profile Security Configurations	Access Controls	X	
TSA-IT-14-06	Weakness in eTAS Access Recertification Process	Access Controls		X
TSA-IT-14-07	FPD and Sunflower Audit Log Reviews	Access Controls	X	
TSA-IT-14-08	Markview Account Termination	Access Controls	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
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