Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit

OIG-14-94

May 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 16, 2014

MEMORANDUM FOR: Luke McCormack
Chief Information Officer

The Honorable Chip Fulghum
Acting Chief Financial Officer

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit.* This report contains comments and recommendations related to information technology internal control deficiencies that were not required to be reported in the Independent Auditors' Report.

We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit of Department of Homeland Security fiscal year 2013 consolidated financial statements. The contract required that KPMG perform its audit according to generally accepted government auditing standards and guidance from the Office of Management and Budget and the Government Accountability Office. KPMG is responsible for the attached management letter dated March 11, 2014, and the conclusion expressed in it.

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

Attachment

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

March 11, 2014

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

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, 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 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.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated December 11, 2013, included internal control deficiencies identified during our audit that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level.

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 and communicated through Notices of Findings and Recommendations (NFRs), are intended to improve internal control or result in other operating efficiencies and are summarized as described below.

With respect to DHS' and components' financial systems' IT controls, we noted certain matters in the areas of security management, access controls, configuration management, segregation of duties, and contingency planning. These matters are described in the *Findings and Recommendations* section of this letter.

The Table of Contents identifies each section of the letter. We have provided a description of key DHS financial systems and IT infrastructure within the scope of the FY 2013 DHS financial statement audit in Appendix A, and a listing of each IT NFR communicated to management in Appendix B.

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 Office of Inspector General and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all weaknesses 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.

DHS' response to the deficiencies identified in our audit is described in page 10 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.

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

Very truly yours,

KPMG LLP

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"). In connection with our audit of the FY 2013 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and IT application controls at DHS Components to assist in planning and performing our audit engagement.

Scope

The scope of our GITC and IT application control test work is described in Appendix A, which provides a description of the key DHS component financial systems and IT infrastructure by DHS Component within the scope of the FY 2013 DHS consolidated financial statement audit.

Approach

General Information Technology Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), formed the basis of our GITC 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 and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs and the IT environment:

- *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.

    - In conjunction with our test work of security management GITCs, limited after-hours physical security testing at select DHS Component facilities was conducted to identify potential control deficiencies in non-technical aspects of IT security.

- *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.

- *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.

    - We performed technical information security testing for key DHS Component network and system devices. The technical security testing was performed from within select DHS facilities

and focused on production devices that directly support DHS' and Components' financial processing and key general support systems.

- *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.

- *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

IT Application Controls

We performed testing over selected key IT application controls 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 application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

Financial Systems Functionality

In recent years, we have noted that the DHS' financial system functionality may be inhibiting the agency's ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting at some Components. At most Components, the financial systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2013, we continued to evaluate and consider the impact of financial system functionality over financial reporting.

SUMMARY OF FINDINGS

During our FY 2013 assessment of GITCs and IT application controls, we noted that the DHS Components made progress in the remediation of IT findings we reported in FY 2012. As a result, we closed 62 (45 percent) of the prior year IT findings which were subject to follow-up procedures in FY 2013. We also issued 32 new findings, which is a significant decrease compared to the 103 new findings in FY 2012.

In FY 2013, we issued 103 total findings, of which approximately 69 percent are repeated from last year. Approximately 35 percent of our repeat findings were for IT deficiencies that management represented were corrected during FY 2013. The new findings in FY 2013 resulted both from additional IT systems and business processes within the scope of our audit this year and from control deficiencies identified in areas which were effective in previous years, and were noted at all DHS components. Customs and Border Protection (CBP) and the Federal Law Enforcement Training Center (FLETC) had the greatest number of new findings. We also considered the effects of financial system functionality when testing internal controls and evaluating findings. Many key DHS financial systems are not compliant with the financial management systems requirements of the *Federal Financial Management Improvement Act of 1996* and Office of Management and Budget (OMB) Circular Number A-127, *Financial Management Systems*, as revised. DHS financial system functionality limitations add substantially to the Department's challenges of addressing systemic internal control weaknesses and limit the Department's ability to leverage IT systems to effectively and efficiently process and report financial data.

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

1. Excessive unauthorized access to key DHS financial applications, resources, and facilities;
2. Configuration management controls that are not fully defined, followed, or effective;
3. Security management deficiencies in the areas of security authorization and role-based security training;
4. Contingency planning that lacked current and tested contingency plans developed to protect DHS resources and financial applications;
5. Lack of proper segregation of duties for roles and responsibilities within financial systems; and
6. Ineffective IT application controls.

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, these deficiencies negatively 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. GAO. The IT findings were combined into one material weakness regarding *IT Controls and Financial System Functionality* for the FY 2013 audit of the DHS consolidated financial statements. Specific results of

GITC and IT application controls test work is provided in separate limited distribution IT management letters provided to component management and the Office of Inspector General.

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

FINDINGS AND RECOMMENDATIONS

Findings

In FY 2013, a number of IT and financial system functionality deficiencies were identified at DHS. Our findings, which were a cross-representation of GITC and financial systems functionality deficiencies identified throughout the Department's Components, follow:

Deficiencies Related to GITCs

Security Management

- Required security authorization activities and supporting artifacts for key financial systems were not always completed and documented.

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

- Federal employees and contractors did not consistently adhere to DHS and Component policies, guidance, and security awareness training concerning the protection of sensitive assets and information from unauthorized access or disclosure.

Access Controls

- Policies and procedures for key financial applications had not been developed to identify elevated access at the application level.

- Management of application, database, network, and remote user accounts was inadequate or inconsistent.

- Safeguards over logical and physical access to sensitive facilities and resources were not always effective.

- Generation, review, and analysis of system audit logs were not always adequate or consistent.

- Access of authorized personnel to sensitive areas containing key financial systems was sometimes more than needed, and data center access controls were not properly enforced.

- Transferred and/or terminated employees were not always timely removed from financial systems, and policies related to revocation of system access were not always implemented or finalized.

Configuration Management

- Configuration management policies and procedures were not always documented.

- Security patch management and configuration deficiencies were identified during the vulnerability assessment on the platforms supporting the key financial applications and general support systems.

- Evidence to support authorized modifications to key financial systems was not always maintained.

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

- Management of administrator access to move IT system code within and between environments was sometimes inadequate or inconsistent.

Segregation of Duties

- Implementation of segregation of duties for IT and financial management personnel with access to financial systems across several platforms was inadequate or incomplete.

Contingency Planning

- Service continuity plans were not always tested, and an alternate processing site was not established for high risk systems.

- Backup policies and procedures were inconsistently documented.

- Backup parameters were not always properly implemented or managed.

Deficiencies Related to Financial Systems Functionality

We noted many cases where financial system functionality was inhibiting DHS' ability to implement and maintain internal controls, notably IT application controls supporting financial data processing and reporting. Financial system functionality limitations also contribute to other control deficiencies and compliance findings presented in our *Independent Auditor's Report*. We noted persistent and pervasive financial system functionality conditions at all of the significant DHS Components in the following general areas:

- At one Component, IT systems have unique functionality issues due to numerous variables, most of which were not within the control of the Component. Production versions of financial systems were outdated and did not provide the necessary core functional capabilities. The Component had installed extensive workarounds, redundant and overlapping systems, and numerous manual reconciliation processes, as necessary to produce auditable financial statements. Some of these workarounds and systems were installed as the only means to validate actual data in the various general ledgers, and support the financial statements. In many cases, the IT systems were not designed to allow the Component to install and use routine automated controls to assist with efficient, reliable, financial processing.

- At another Component, multiple financial IT systems continued to be impaired by functionality limitations which prevent implementation of effective security controls. These limitations, which

principally impact audit logging controls intended to monitor logical access and configuration management activities, were being addressed through enterprise-wide solutions which were not fully implemented at the time of our audit procedures. Additionally, certain feeder systems were operating with outdated and unsupported system software components which exposed them to vulnerabilities that cannot be mitigated.

- Several financial systems have limited capacity to process, store, and report financial and performance data to facilitate decision making, safeguarding and management of assets, and prepare financial statements that comply with Generally Accepted Accounting Principles.

- One financial system lacked the controls necessary to prevent or detect and correct excessive drawback claims. Specifically, the programming logic for the system did not link drawback claims to imports at a detailed, line item level.

- Technical configuration limitations, such as outdated systems that were no longer fully supported by the software vendors, impaired DHS' ability to fully comply with policy in areas such as IT security controls, notably password management, audit logging, user profile changes, and the restricting of access for off-boarding employees and contractors.

- System capability limitations prevent or restrict the use of applications controls to replace less reliable, more costly manual controls; or in some cases, required additional manual controls to compensate for IT security or control weaknesses.

- Some IT subsidiary modules that could improve controls and reliability were not active due to various system design and integrity reasons.

- Some IT system controls were not designed to prevent the receipt of goods and services in excess of available funding.

Cause/Effect

DHS management recognized the need to upgrade its financial systems. Until serious legacy IT issues are addressed and updated IT solutions implemented, compensating controls and other complex manual workarounds must support its IT environment and financial reporting. As a result, DHS' difficulty attesting to a strong control environment, to include 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 manner to ensure accuracy, confidentiality, integrity, and availability. Some of the weaknesses may result in material errors in DHS' financial data that were not detected in a timely manner through the normal course of business. In addition, because of the presence of IT control and financial system functionality weaknesses; there is added pressure on mitigating controls to operate effectively. Because mitigating controls were often more manually focused, there is an increased risk of human error that could materially affect the financial statements.

Recommendation

We recommend that the DHS Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO), in coordination with DHS Component management, continue the *Financial Systems Modernization* initiative, and make necessary improvements to the Department's financial management systems and supporting IT security controls.

Specific recommendations were provided in separate letters provided to DHS Component management.

MANAGEMENT RESPONSE

The DHS Office of Inspector General discussed our report with DHS management and 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 Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit

Below is a description of key financial management systems and supporting IT infrastructure included in the scope of the DHS FY 2013 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 and is hosted on the DHS OneNet at the Stennis Data Center in Mississippi (MS).

Customs and Border Protection (CBP)

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

SAP is CBP's financial system of record. SAP is a major integrated client/server-based financial management system implemented by CBP 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. The SAP instance includes several modules (including ECC 6.0, Intelligent Procurement, and Budget Tools) 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 functionality, among others. The SAP ECC financial management system was included within the scope of the FY 2013 financial statement audit. The Border Enforcement and Management Systems (BEMS) Program Office and the Enterprise Data Management and Engineering (EDME) Program Office own the SAP application, UNIX and Windows operating systems and Oracle database located in Virginia (VA).

Automated Commercial Environment (ACE)

ACE is the commercial trade processing system being developed and implemented by CBP to replace the Automated Commercial System (ACS). The mission of ACE is to implement a secure, integrated, government-wide system for the electronic collection, use, and dissemination of international trade and transportation data essential to Federal agencies. ACE is a custom-developed, internet-facing, multi-tier system with high availability characteristics, and it processes sensitive data. ACE is being deployed in phases over several years. As a result, some financial modules will remain in the ACS operating environment until they can be developed and deployed in ACE. Since ACE was partially implemented during FY2013, it was included within the scope of the FY 2013 financial statement audit. The Cargo Systems Program Office (CSPO), the Enterprise Networks and Technology Support (ENTS) Program Office and the EDME Program Office own the ACE application, AIX operating system and DB2 database located in VA.

Automated Commercial System (ACS)

ACS is a collection of seven mainframe-based sub-systems used by the CBP 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. ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, and provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations, illegal imports and terrorist activities. The ACS system was included within the scope of the FY 2013 financial statement audit. The CSPO and the ENTS Program Office own the ACS application and mainframe located in VA.

District of Columbia Metropolitan Local Area Network (DC Metro LAN)

The DC Metro LAN provides CBP's DC area employees and contractors user access to enterprise-wide applications and systems. The mission of the DC Metro LAN is to support the mission of CBP operational elements in the DC Metro LAN region of the organization. The boundary of the DC Metro LAN includes tools such as personal computers, laptop computers, printers and file/print servers which enable CBP officers and agents to interact with all other applications and systems in the CBP environment. The DC Metro LAN supports ACE, ACS, and SAP and provides authentication mechanisms that are used by SAP for single sign on capability; as a result, the DC Metro LAN was included within the scope of the FY 2013 financial statement audit. The Field Support (FS) Program Office and the EDME Program Office own the DC Metro LAN located in VA.

United States Coast Guard (USCG or Coast Guard)

Core Accounting System (CAS)

CAS is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. CAS is hosted at the Coast Guard Finance Center (FINCEN) in VA. CAS interfaces with the Financial and Procurement Desktop (FPD), also located at FINCEN. CAS is used by financial management individuals as CAS is the main system of record for financial information. CAS has a Hewlett-Packard (HP) UNIX operating system with an Oracle database, and the organizations responsible for CAS are FINCEN, Coast Guard OCFO, and Coast Guard OCIO.

Financial Procurement Desktop (FPD)

The FPD application is used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is located at the FINCEN in VA, and has an HP UNIX operating system and Oracle database. The organizations responsible for CAS are FINCEN, Coast Guard OCFO, and Coast Guard OCIO.

Joint Uniform Military Pay System (JUMPS)

JUMPS is an IBM zOS mainframe application and database that is used for paying USCG active and reserve payroll and is mainly used by Pay and Personnel Center (PPC) employees. JUMPS is located at the Burlington Northern Santa Fe data center in Kansas. The responsible organization for JUMPS is PPC, which falls under the purview of the Coast Guard OCIO.

Direct Access

Direct Access is the system of record for all functionality, data entry, and processing of payroll events for the Coast Guard. Every Coast Guard employee is a user of the system. Employees may use Direct Access to correct their own personal information, such as address and beneficiaries. The main financial users use Direct Access to process payroll events and change personnel records such as pay scales. Up until June 2013, Direct Access was maintained by IBM Application On Demand (IBM AOD) in the iStructure data center facility in Arizona (AZ) with an automated backup site located in a Qwest data center in VA. Starting in June 2013, Direct Access is maintained by Addx Corporation and is located in VA. Direct Access is a PeopleSoft application residing on servers operating the Solaris and Windows Server 2000 operating systems and is supported by an Oracle database. The responsible organization for Direct Access is the Office of the Chief Information Officer (OCIO).

Global Pay (Direct Access II)

Global Pay provides retiree and annuitant support services. Until June 2013, Global Pay was maintained by IBM AOD in the iStructure data center facility in AZ with an automated backup site located in a Qwest data center in VA. Starting in June 2013, Global Pay is maintained by Addx Corporation and is located in VA. Global Pay is a PeopleSoft application residing on servers operating the IBM x Series operating system and is supported by an Oracle database. The responsible organization for Global Pay is the Coast Guard OCIO.

Naval and Electronics Supply Support System (NESSS)

NESSS is one of four automated information systems that comprise the family of Coast Guard logistics systems. NESSS is a fully integrated system linking the functions of provisioning and cataloging, unit configuration, supply and inventory control, procurement, depot-level maintenance and property accountability, and a full financial general ledger. NESSS is used by both financial and logistics personnel across numerous Coast Guard locations. NESSS is located at the Operations Systems Center (OSC) in West Virginia, resides on servers operating the Microsoft Windows 2003 and HP/UNIX operating systems, and is supported by an Oracle database. The responsible organizations for NESSS are the Office of Logistics Program Management and OSC, which act under the purview of the Coast Guard OCIO.

Aviation Logistics Management Information System (ALMIS)

ALMIS provides Coast Guard Aviation logistics management support in the areas of operations, configuration management, maintenance, supply, procurement, financial, and business intelligence. Additionally, ALMIS covers the following types of information: Financial, Budget, Planning, Aircraft & Crew Status, Training & Readiness, and Logistics & Supply. The Aviation Maintenance Management Information System, a subcomponent of ALMIS, functions as the inventory management/fiscal accounting component of the ALMIS application. The Aircraft Repair & Supply Center Information Systems Division in North Carolina (NC) hosts the ALMIS application. ALMIS is used by both financial and logistics personnel across numerous Coast Guard locations. ALMIS is located at the Aviation Logistics Center (ALC) in NC and has a HP UNIX operating system and a Haley database. The responsible organization for ALMIS is ALC.

United States Citizenship and Immigration Services (USCIS)

Federal Financial Management System (FFMS)

The FFMS is a CFO designated financial system and certified software application that conforms to OMB Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS is a commercial off-the-shelf (COTS) financial reporting system, which has an IBM z/OS operating system and an Oracle database. It includes the core system used by accountants, FFMS Desktop that is used by end-users, and a National Finance Center (NFC) payroll interface. The FFMS mainframe component and servers are hosted at the DHS Enterprise Data Center (DC-2) located in VA. U.S. Immigration and Customs Enforcement (ICE) is the system owner and manages FFMS for USCIS.

USCIS Network (CIS1)

CIS1 is the Active Directory Domain Services Platform used within the USCIS that contains all of USCIS's Active Directory and Exchange resources. CIS1 is a part of the Enterprise Infrastructure Services accreditation boundary and all Active Directory information, including the Active Directory database itself, is hosted on specified servers called Domain Controllers. These 52 Active Directory Domain Controllers are located throughout the country, with the majority of them being located in VA and Nebraska.

Federal Emergency Management Agency (FEMA)

Integrated Financial Management Information System (IFMIS)

IFMIS is the official accounting system of FEMA and maintains all financial data for internal and external reporting. IFMIS is comprised of five subsystems: Funding, Cost Posting, Disbursements, Accounts Receivable, and General Ledger. The application is a COTS software package developed and maintained by Digital Systems Group Incorporated. IFMIS interfaces with the Payment and Reporting System (PARS), the Emergency Support System (ES), ProTrac, Smartlink (Department of Health and Human Services [HHS]), Treasury Information Executive Repository (Department of the Treasury), Secure Payment System (Department of the Treasury), Grants Management System (Department of Justice), United States Coast Guard Credit Card System, Credit Card Transaction Management System (CCTMS), Assistance to Firefighters Grants, eGrants, and Enterprise Data Warehouse and Payroll (Department of Agriculture NFC). The IFMIS production environment is located in VA.

Payment and Reporting System (PARS)

PARS is a standalone web-based application. The PARS database resides on the IFMIS UNIX server and is incorporated within the certification & accreditation boundary for that system. Through its web interface, PARS collects Standard Form 425 information from grantees and stores the information in its Oracle 9i database. Automated scheduled jobs are run daily to update and interface grant and obligation information between PARS and IFMIS. PARS is located in VA.

Non-Disaster Grant Management System (NDGrants)

NDGrants is a web-based system that supports the grants management lifecycle and is used by external stakeholders and grantees, via a public Web site, to apply for grants and monitor the progress of grant applications and payments and view related reports, and by the FEMA Grants Program Directorate, Program Support Division, via an internal Web site, for reviewing, approving, and processing grant awards. NDGrants interfaces with two other systems: FEMA's internal Integrated Security and Access Control System (ISAAC), a component of the Network Access Control System used for user credentialing and role-based access; and the HHS Grants.gov system, used for publishing grant solicitations and downloading applications. NDGrants is located in VA.

Emergency Management Mission Integrated Environment (EMMIE)

EMMIE is an internal Web-based grants management solution used by FEMA program offices and user communities directly involved in the grant lifecycle associated with the Public Assistance Grant Program and the Fire Management Assistance Grant Program. It is also designed to interface with other government entities and grant and sub-grant applicants (e.g., states and localities). EMMIE provides functionality for public entities and private-non-profit entities to create and submit grant applications and for FEMA users to review and award applications, generate and review relevant mission critical reports, process amendments, and conduct close-out activities. Interfaces exist between the EMMIE system, IFMIS, and ISAAC. EMMIE is located in VA.

Emergency Support (ES)

ES is an internal FEMA application for pre-processing disaster-related financial transactions, including allocation, commitment, obligation, mission assignment, and payment requests from other internal and external systems. ES serves as the primary interface to IFMIS. It also allows FEMA users to process disaster housing payments, perform payment recoupment, and conduct other administrative tasks. In addition to IFMIS, ES has interfaces to several other FEMA systems, including:

- ISAAC (organizational and personnel data and team setup);
- Emergency Coordination (incident and disaster declarations);
- Enterprise Coordination and Approvals Processing System (commitment and mission assignment [obligation] requests);
- Hazard Mitigation Grants Program (allocation and obligation requests);
- Individual Assistance (payment and recoupment requests);
- Public Assistance (obligation and allocation requests);
- Automated Deployment Database (personnel data);
- Assistance to Firefighters Grants (obligation, invoice, and vendor requests);
- EMMIE (obligation requests);
- Mitigation Electronic Grants Management System (obligation requests); and
- CCTMS (expenditure requests).

ES is located in Virginia.

Traverse

Traverse is the general ledger application currently used by the National Flood Insurance Program (NFIP) Bureau and Statistical Agent to generate the NFIP financial statements. Traverse is a client-server application that runs on the NFIP Local Area Network (LAN) Windows server environment located in Maryland (MD). The Traverse client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members and interfaces with a Microsoft Structured Query Language database hosted on an internal segment of the NFIP LAN. Traverse has no known external system interfaces.

Transaction Recording and Reporting Processing (TRRP)

The TRRP application acts as a central repository of all data submitted by the Write Your Own (WYO) companies and the Direct Servicing Agent (DSA) for the NFIP. TRRP also supports the WYO program, primarily by ensuring the quality of financial data submitted by the WYO companies and DSA to TRRP. TRRP is a mainframe-based application that runs on the NFIP mainframe logical partition in Connecticut. TRRP has no known system interfaces.

Federal Law Enforcement Training Center (FLETC)

Financial Accounting and Budgeting System (FABS)

The FLETC FABS application (also referred to as Momentum) is an all-in-one financial processing system. It functions as the computerized accounting and budgeting system for FLETC. FLETC provides financial management services to the Office of Intelligence and Analysis and the Office of Operations Coordination and Planning (IA&OPS) through a separately hosted Momentum environment, which was developed to mirror the FLETC Momentum environment. The FABS system exists to provide all of the financial and budgeting transactions in which FLETC is involved. FABS system users are from all FLETC sites that input requisitions and managers that approve receipt of property and manage the property asset records and financial records for contracts, payments, payroll, and budgetary transactions. Hosted on a Microsoft Server 2003 and Oracle Linux Server, the FABS application (Oracle Web Logic) and database (Oracle 10g) servers reside on the FLETC Glynco Administrative Network (GAN) in a Hybrid physical network topology and are accessible from four sites: Georgia (GA), DC, New Mexico, and MD. The system owner and responsible office is the Finance Division Chief in the FLETC OCFO.

Glynco Administrative Network (GAN)

The purpose of GAN is to provide access to IT network applications and services to include video and voice teleconferencing to authorized FLETC personnel, contractors and partner organizations located at the Georgia facility. It provides authorized users access to email, internet services, required applications such as Financial Management Systems, Procurement systems, Property management systems, Video conference, and other network services and shared resources. The GAN is located in GA and is owned and operated by the FLETC OCIO.

United States Immigration and Customs Enforcement (ICE)

Federal Financial Management System (FFMS)

The FFMS is a CFO designated financial system and certified software application that conforms to OMB Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS is a COTS financial reporting system, which has an IBM z/OS operating system and an Oracle database. It includes the core system used by accountants, FFMS Desktop that is used by average users, and a National Finance Center payroll interface. The FFMS mainframe component and servers are hosted at DC-2 in VA. The ICE OCIO is responsible for FFMS.

ICE Network (ADEX)

The ICE Network, also known as the ADEX E-mail System, is a major application for ICE. The ADEX servers and infrastructure for the headquarters and National Capital Area are located in MS and VA. ADEX currently interfaces with the Diplomatic Telecommunications Service Program Office ICENet Infrastructure.

Transportation Security Administration (TSA)

Core Accounting System (CAS)

CAS is the core accounting system that records financial transactions and generates financial statements for TSA. CAS is hosted at the Coast Guard's FINCEN in VA. CAS interfaces with other systems located at the FINCEN, including the Financial Procurement Desktop (FPD) and Sunflower. CAS is used by financial management individuals as CAS is the main system of record for financial information. CAS is comprised of an HP UNIX operating system and an Oracle database.

Financial Procurement Desktop (FPD)

The FPD application is used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD interfaces with the CAS system and is hosted at the FINCEN in VA. FPD is comprised of an HP UNIX operating system and an Oracle database.

Sunflower

Sunflower is a customized third-party COTS product used for TSA and Federal Air Marshal Service property management. Sunflower interacts directly with the Office of Finance Fixed Assets module in CAS and interfaces with the FPD system. Sunflower is hosted at the FINCEN in VA. Sunflower is comprised of a Red Hat Linux operating system and an Oracle database.

Electronic Time Attendance and Scheduling (eTAS)

eTAS is an automated and standardized labor management solution. The system provides an automated means to schedule employee work and leave hours, record hours worked and not worked, and provide bi-weekly time records to TSA's payroll provider, the NFC. The system automates the workforce management process to reduce the amount of time, effort, and associated cost required for entry of data. eTAS is comprised of a Windows 2003 operating system and an Oracle database, and is located at DC-2 in VA. The Office of Human Capital is responsible for eTAS.

Appendix B

FY 2013 IT Notices of Findings and Recommendations at DHS

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

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-13-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at DHS	Security Management		X
OCIO-IT-13-01	Inadequate Recertification of DC-2 Physical Access	Access Controls		X
OCIO-IT-13-02	Backup Log Rotation Not Consistently Performed	Contingency Planning	X	
OCIO-IT-13-03	Inadequate Recertification of DHS Enterprise Data Center 1 Physical Access	Access Controls	X	

Customs and Border Protection

FY 2013 NFR #[1]	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-13-01	Inappropriately Configured Password Parameters for SAP UNIX Operating System (OS)	Access Controls	X	
CBP-IT-13-02	Audit Activity Logs Not Reviewed for SAP Oracle Database (DB)	Access Controls		X
CBP-IT-13-03	Lack of Review of SAP Windows OS Accounts	Access Controls		X
CBP-IT-13-04	Incomplete SAP UNIX OS Backups	Contingency Planning	X	
CBP-IT-13-05	Lack of Evidence of Review of SAP UNIX OS Audit Logs	Access Controls	X	
CBP-IT-13-06	Lack of Review of ACS Application Audit Logs	Access Controls		X
CBP-IT-13-07	Security Awareness Issues Identified during After-Hours Physical Security Testing at CBP	Security Management		X
CBP-IT-13-08	Lack of Review of Developer Access to the ACS Production Application Data	Access Controls		X
CBP-IT-13-09	Inappropriately Configured ACE AIX OS Password Parameters	Access Controls	X	
CBP-IT-13-10	Inappropriately Configured ACE DB2 Database Password Parameters	Access Controls	X	
CBP-IT-13-11	Lack of Functionality in the ACS	Business Process Controls		X
CBP-IT-13-12	Lack of Review of ACE DB2 Database Accounts	Access Controls	X	
CBP-IT-13-13	Lack of Annual Recertification of Mainframe Privileged Users	Access Controls		X

[1] NFR numbers CBP-IT-13-15, CBP-IT-13-21, CBP-IT-13-26, CBP-IT-13-27 and CBP-IT-13-32 were intentionally omitted from sequence.

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-13-14	Incomplete Raised Floor Visitors Logs	Access Controls	X	
CBP-IT-13-16	Weaknesses in Creating New DC Metro LAN Accounts	Access Controls		X
CBP-IT-13-17	Separated Personnel on SAP Application User Listing	Access Controls		X
CBP-IT-13-18	Weaknesses in Creating New ACE Accounts	Access Controls		X
CBP-IT-13-19	Weaknesses in Creating New ACS Accounts	Access Controls		X
CBP-IT-13-20	SAP Configuration Baseline Weaknesses	Configuration Management	X	
CBP-IT-13-22	Separated Personnel on Mainframe User Listing	Access Controls		X
CBP-IT-13-23	Weaknesses in Documenting New ACE User Accounts in the Development and Testing Environments	Configuration Management	X	
CBP-IT-13-24	ACS Segregation of Duties Weaknesses over the Production Environment	Access Controls		X
CBP-IT-13-25	Lack of Unique Account Identifiers for ACS	Access Controls	X	
CBP-IT-13-28	ACS Application Recertification Weaknesses	Access Controls	X	
CBP-IT-13-29	Audit Activity Logs Not Generated or Reviewed for SAP Windows OS	Access Controls	X	
CBP-IT-13-30	Separated Personnel on DC Metro LAN User Listing	Access Controls		X
CBP-IT-13-31	Separated Personnel on ACE Application User Listing	Access Controls		X
CBP-IT-13-33	Contractor Separation Process Weaknesses	Security Management		X
CBP-IT-13-34	Weaknesses over the Employee Separation Process	Security Management		X

United States Coast Guard

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-13-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Access Controls		X
CG-IT-13-02	Weakness in Direct Access Audit Logs and Segregation of Duties	Access Controls		X
CG-IT-13-03	Weakness in Direct Access Annual User Recertification	Access Controls		X
CG-IT-13-04	Security Awareness Issues Identified During Social Engineering Testing at Surface Forces Logistics Center	Security Management		X
CG-IT-13-05	Security Awareness Issues Identified during After-Hours Physical Security Testing at the Surface Forces Logistics Center, OSC, ALC, and FINCEN	Security Management		X
CG-IT-13-06	Access and Configuration Management Controls - Vulnerability Assessment	Configuration Management		X
CG-IT-13-07	Weakness in JUMPS Annual User Recertification	Access Controls	X	
CG-IT-13-08	Weakness in NESSS Annual User Recertification	Access Controls		X

United States Citizenship and Immigration Services

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-13-01	Security Awareness Issues Identified During Social Engineering Testing at USCIS	Security Management		X
CIS-IT-13-02	Deficiencies in transferred/terminated employee exit processing	Access Controls		X
CIS-IT-13-03	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-13-04	Weakness in CIS1 Password Complexity	Access Controls	X	
CIS-IT-13-05	FFMS Vulnerability Weaknesses Impact USCIS Operations	Configuration Management		X

Federal Emergency Management Agency

FY 2013 NFR #	NFR Title	FISCAM Control Area(s)	New Issue	Repeat Issue
FEMA-IT-13-01	Non-Compliance with Alternate Processing Site Requirements for Key Financial Systems	Contingency Planning		X
FEMA-IT-13-02	Insufficient Audit Log Controls for Key Financial Systems	Access Controls		X
FEMA-IT-13-03	Inconsistent Implementation of DHS Background Investigation Requirements for FEMA Federal Employees and Contractors	Security Management		X
FEMA-IT-13-04	Incomplete Implementation of Role-Based Training for Individuals with Significant Information Security Responsibilities	Security Management		X
FEMA-IT-13-05	Non-Compliant Security Authorization Package for NDGrants	Security Management		X
FEMA-IT-13-06	Non-Compliance with DHS and FEMA Password Requirements for Oracle Databases Supporting Certain Financial Applications	Access Controls		X
FEMA-IT-13-07	Incomplete Exception Request for Password Controls on Oracle Databases Supporting Certain Financial Applications	Security Management[2]		X
FEMA-IT-13-08	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-13-09	Weaknesses Identified during the Vulnerability Assessment on IFMIS	Access Controls; Configuration Management		X
FEMA-IT-13-10	Weaknesses Identified during the Vulnerability Assessment on the NFIP LAN	Access Controls; Configuration Management		X

[2] NFR FEMA-IT-13-07 was reported in conjunction with FEMA-IT-13-06 as part of GITC deficiencies related to access controls in our *Independent Auditors' Report* dated December 11, 2013.

FY 2013 NFR #	NFR Title	FISCAM Control Area(s)	New Issue	Repeat Issue
FEMA-IT-13-11	Weaknesses Identified during the Vulnerability Assessment on Financially Significant Segments of the FEMA Enterprise Network and End-User Computing Environment	Configuration Management		X
FEMA-IT-13-12	Weaknesses Identified during the Vulnerability Assessment on EMMIE	Configuration Management		X
FEMA-IT-13-13	Weaknesses Identified during the Vulnerability Assessment on NDGrants	Access Controls; Configuration Management		X
FEMA-IT-13-14	Non-Compliant Security Authorization Package for ES	Security Management		X
FEMA-IT-13-15	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for EMMIE, NDGrants, and ES	Configuration Management		X
FEMA-IT-13-16	Incomplete Account Management Documentation for the EMMIE Application	Access Controls	X	
FEMA-IT-13-17	Incomplete Account Management Documentation for NDGrants	Access Controls		X
FEMA-IT-13-18	Incomplete Account Management Documentation for ES	Access Controls		X
FEMA-IT-13-19	Excessive or Inappropriate Access to IFMIS	Access Controls; Segregation of Duties		X
FEMA-IT-13-20	Lack of EMMIE System Owner Approval for Database Accounts	Access Controls		X
FEMA-IT-13-21	Lack of ES System Owner Approval for Database Accounts	Access Controls		X
FEMA-IT-13-22	Lack of NDGrants System Owner Approval for Database Accounts	Access Controls		X
FEMA-IT-13-23	Inconsistent Authorization of New and Modified IFMIS Application User Access	Access Controls		X
FEMA-IT-13-24	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems	Configuration Management		X
FEMA-IT-13-25	Inconsistent Activities and Incomplete Documentation Supporting Configuration Changes for the IFMIS Application	Configuration Management		X

FY 2013 NFR #	NFR Title	FISCAM Control Area(s)	New Issue	Repeat Issue
FEMA-IT-13-26	Inconsistent Review of IFMIS Audit Logs	Access Controls		X
FEMA-IT-13-27	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the IFMIS Production Environment	Configuration Management		X
FEMA-IT-13-28	Non-Compliant Security Authorization Package for IFMIS	Security Management	X	

Federal Law Enforcement Training Center
and Intelligence & Analysis and Operations (IA&OPS)

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-13-01	FLETC Momentum Audit Log Reviews not Consistently Maintained	Access Controls	X	
FLETC-IT-13-02	Weakness in GAN Password Complexity	Access Controls	X	
FLETC-IT-13-03	FLETC Momentum Account Management not Consistently Performed	Access Controls	X	
FLETC-IT-13-04	Momentum Application Inactivity Lockout is not Appropriately Configured	Access Controls	X	
FLETC-IT-13-05	FLETC Contractor Separation not Fully Monitored	Access Controls	X	
IAOPS-IT-13-01	IA&OPS Momentum Audit Log Reviews not Consistently Performed in a Timely Manner	Access Controls	X	
IAOPS-IT-13-02	IA&OPS Segregation of Duties not Fully Enforced	Segregation of Duties	X	
IAOPS-IT-13-03	IA&OPS Momentum Account Management not Consistently Performed	Access Controls		X
IAOPS-IT-13-04	Momentum Application Inactivity Lockout is not Appropriately Configured	Access Controls	X	
IAOPS-IT-13-05	IA&OPS Contractor Separation not Fully Monitored	Access Controls	X	
IAOPS-IT-13-06	Multiple Payment Vouchers can be Processed Against the Same Invoice	Business Process Controls	X	

United States Immigration and Customs Enforcement

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-13-01	Weakness in FFMS Backup Documentation	Contingency Planning	X	
ICE-IT-13-02	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-IT-13-03	Weakness in FFMS Segregation of Duties Relating to IT Functions	Segregation of Duties	X	
ICE-IT-13-04	Weakness in implementation of procedures for transferred/terminated employee and contractor exit processing	Access Controls		X
ICE-IT-13-05	Inadequate FFMS User Access Request Forms	Access Controls		X
ICE-IT-13-06	FFMS network and servers were installed with default configuration settings and protocols	Configuration Management		X
ICE-IT-13-07	FFMS Mainframe Production databases were installed and configured without baseline security configurations	Configuration Management		X
ICE-IT-13-08	FFMS servers have inadequate patch management	Configuration Management		X
ICE-IT-13-09	Weakness in ADEX Password Complexity	Access Controls	X	

National Protection and Programs Directorate

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
NPPD-IT-13-01	Security Awareness Issues Identified During Social Engineering Testing at NPPD	Security Management		X
NPPD-IT-13-02	Security Awareness Issues Identified during After-Hours Physical Security Testing at NPPD	Security Management		X

Transportation Security Administration

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-13-01	Weakness in eTAS user recertification	Access Controls		X
TSA-IT-13-02	Weakness in eTAS password complexity	Access Controls		X
TSA-IT-13-03	Weakness in eTAS Restoration Testing of Backups	Contingency Planning		X
TSA-IT-13-04	Weakness in eTAS review of audit logs	Access Controls		X
TSA-IT-13-05	eTAS System User Access	Access Controls		X
TSA-IT-13-06	Security Awareness Issues Identified During Social Engineering Testing at TSA Headquarters	Security Management		X[3]
TSA-IT-13-07	Physical Security and Security Awareness Issues Identified During After Hours Testing at TSA Headquarters	Security Management		X3

[3] FY 2012 NFR TSA-IT-12-01 was split into two findings for FY 2013 to report separately on the results of each set of enhanced information security testing procedures performed at TSA.

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy 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 Financial Officer
Chief Information Officer
Chief Information Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

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 (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.