Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2012 Department of Homeland Security Financial Statement Audit

OIG-13-58

April 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 4, 2013

MEMORANDUM FOR: Richard Spires
Chief Information Officer

Peggy Sherry
Chief Financial Officer

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the FY 2012 Department of Homeland Security Financial Statement Audit*

Attached for your action is our final report, *Information Technology Management Letter for the FY 2012 Department of Homeland Security Financial Statement Audit.* The independent accounting firm KPMG LLP (KPMG) performed the audit of Department of Homeland Security (DHS) financial statements as of September 30, 2012, and prepared this information technology (IT) management letter.

KPMG is responsible for the attached IT management letter dated December 20, 2012, and the conclusion expressed in it. We do not express an opinion on DHS' financial statements or internal controls or conclusions on compliance with laws and regulations. The DHS management concurred with all recommendations.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

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

April 2, 2013

Acting Inspector General
U.S. Department of Homeland Security

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

We have audited the balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2012 and the related statements of net cost, changes in net position and custodial activity, and combined statement of budgetary resources for the year then ended (referred to herein as the "fiscal year (FY) 2012 financial statements"). The objective of our audit was to express an opinion on the fair presentation of these financial statements. We were also engaged to examine the Department's internal control over financial reporting of the FY 2012 financial statements, based on the criteria established in Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Internal Control,* Appendix A.

Our *Independent Auditors' Report* issued on November 14, 2012, describes a limitation on the scope of our audit that prevented us from performing all procedures necessary to express an unqualified opinion on the DHS' FY 2012 financial statements and internal control over financial reporting. In addition, the FY 2012 DHS *Secretary's Assurance Statement* states that the Department was able to provide qualified assurance that internal control over financial reporting was operating effectively at September 30, 2012.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 14, 2012, included financial systems general Information Technology (IT) control (GITC) deficiencies which we believe contribute to a DHS-level significant deficiency that is considered a material weakness. IT control deficiencies were identified in areas of access controls, configuration management, security management, contingency planning, and segregation of duties. We also noted that in some cases, financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR). We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key DHS financial systems within the scope of the FY 2012 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls (comments not related to IT) have been presented in a separate letter to the Office of Inspector General (OIG) and the DHS Chief Financial Officer (CFO).

We would be pleased to discuss these comments and recommendations with you at any time. This report is intended for the information and use of the DHS' management, the DHS Office of Inspector General, the U.S. Office of Management and Budget, the U.S. Congress, and the Government Accountability Office, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

During our engagement to perform an integrated audit of DHS, we evaluated the design and effectiveness of general information technology controls (GITCs) of DHS' financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the GAO, formed the basis of our audit as it relates to GITC assessments at DHS.

FISCAM was designed to inform financial 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 audit. FISCAM also provides guidance to IT 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 functions to be essential to the effective operation of GITCs and the IT environment.

- *Security Management (SM)* – 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.
- *Access Control (AC)* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.
- *Segregation of Duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our GITC audit procedures, we also performed technical security testing for key network and system devices at DHS. The technical security testing was performed both over the Internet and from within select DHS facilities, and focused on test, development, and production devices that directly support DHS' financial processing and key general support systems. Limited social engineering and after-hours physical security testing was also included in the scope of the technical security testing at certain DHS components.

In addition, we performed testing over selected key application controls to assess the controls that support DHS 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. Specific results of the application controls test work is provided in separate *For Official Use Only* IT management letters provided to component management and the OIG.

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 2012, we continued to evaluate and consider the impact of financial system functionality over financial reporting.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During our FY 2012 assessment of IT general and application controls, we noted that the DHS components made progress in the remediation of IT findings we reported in FY 2011. As a result, we closed approximately 68 (47 percent) of our prior year IT findings. However, we identified 103 new findings, which is a significant increase compared to the 41 new findings in FY 2011. In FY 2012, we identified approximately 180 total findings, of which approximately 43 percent are repeated from last year. Approximately 41 percent of our repeat findings were for IT deficiencies that management represented were corrected during FY 2012. The new findings in FY 2012 resulted primarily from additional IT systems and business processes within the scope of our audit this year, and were noted at all DHS components. Customs and Border Protection (CBP) and the Federal Emergency Management Agency (FEMA) 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 Federal Financial Management Improvement Act of 1996 (FFMIA) and 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 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 area of the certification and accreditation process and an ineffective program to enforce role-based security training and staff background investigations;
4. contingency planning that lacked current, tested, contingency plans developed to protect DHS resources and financial applications; and
5. lack of proper segregation of duties for roles and responsibilities within financial systems.

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 (AICPA) and the GAO. The IT findings were combined into one material weakness regarding IT Controls and Financial System Functionality for the FY 2012 audit of the DHS consolidated financial statements.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

In FY 2012, a number of IT and financial system functionality deficiencies were identified at DHS. Approximately 180 findings were identified of which approximately 43 percent are repeated from last year. The primary (circle) bullets listed below each FISCAM heading are a cross-representation of the nature of IT general control deficiencies identified throughout the Department's components. The secondary (dash) bullets represent single or multiple occurrence findings in one or more components.

Findings:

Our findings related to GITCs and financial systems functionality follow:

Related to IT Financial Systems Controls

1. *Access Controls*:

   - Deficiencies in management of application and/or database accounts, network, and remote user accounts.
   - Ineffective safeguards over logical and physical access to sensitive facilities and resources.
   - Lack of generation, review, and analysis of system audit logs and adherence to DHS requirements.
   - Excessive access of authorized personnel to sensitive areas containing key financial systems, and lack of proper enforcement of data center access controls.

2. *Configuration Management*

   - Lack of documented policies and procedures.
   - Lack of sufficiently documented script management test plans in accordance with minimum DHS requirements.
   - Security patch management and configuration deficiencies identified during the vulnerability assessment on the platforms supporting the key financial applications and general support systems.
   - Lack of maintained evidence to support authorized modifications to key financial systems.
   - Internal requirements to conduct Functional Configuration Audits and Physical Configuration Audits were not followed at one component.

3. *Security Management:*

   - Systems certification and accreditation were not completed and documented.
   - IT Security personnel lack mandatory role-based training or compliance was not documented and monitored, and computer security awareness training was not monitored.
   - Background investigations of Federal employees and contractors employed to operate, manage and provide security over IT systems were not being properly conducted, nor consistently tracked and monitored.

4. *Contingency Planning:*

- Service continuity plans were not tested nor updated to reflect the current environment, and an alternate processing site has not been established for high risk systems.
- Authorized access to backup media was not periodically reviewed and updated; at one component procedures to periodically test backups was not implemented.

5. *Segregation of Duties:*

- Lack of evidence to show that least privilege and segregation of duties controls exist, including policies and procedures to define conflicting duties and access rights.

These control findings, including other significant deficiencies and criteria are described in greater detail in separate *For Official Use* Only letters provided to DHS management.

Related to Financial System Functionality

Coast Guard (some conditions impact the Transportation Security Administration (TSA) as a user of Coast Guard's IT accounting systems):

- The core financial system configuration management process relies on an IT script process as a solution primarily to compensate for system functionality and data quality issues.
- The component is unable to routinely query its various general ledgers to obtain a complete population of financial transactions, and consequently must create many manual custom queries that delay financial processing and reporting processes.
- A key financial system is limited in processing overhead cost data and depreciation expenses in support of the property, plant and equipment financial statement line item.
- Production versions of financial systems are outdated and do not provide the necessary core functional capabilities (e.g., general ledger capabilities).
- The budgetary module of the core financial system is not activated. As a result, key attributes (e.g., budget fiscal year) are missing and potential automated budgetary entries (e.g., upward adjustments) are not used. This has created the need for various manual workarounds and non-standard adjustments (i.e., topsides) to be implemented.
- Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls that would improve accuracy, reliability, and facilitate efficient processing of certain financial data such as:
  - Receipt of goods and services upon delivery. As a result, the Coast Guard records a manual estimate of potential receipted goods and services at year end in the general ledger;
  - Ensuring proper segregation of duties and access rights, such as automating the procurement process to ensure that only individuals who have proper contract authority can approve transactions or setting system access rights within the fixed asset subsidiary ledger;
  - Maintaining adequate posting logic transaction codes to ensure that transactions are recorded in accordance with generally accepted accounting principles (GAAP); and

- Tracking detailed transactions associated with intragovernmental business and eliminating the need for default codes such as Trading Partner Identification Number that cannot be easily researched.

Other Department Components:

We noted many cases where financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT application controls supporting financial data processing and reporting. We noted persistent and pervasive financial system functionality conditions at all of the significant DHS components in the following general areas:

- Inability of financial systems 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 GAAP.
- Technical configuration limitations, such as outdated systems that are 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, require additional manual controls to compensate for IT security or control weaknesses.

Cause/Effect: DHS management recognizes 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 in attesting to a strong control environment, to include effective general IT controls and reliance on key financial systems, will 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 are not detected in a timely manner through the normal course of business. In addition, because of the presence of IT control and financial system functionality weaknesses; there is added pressure on mitigating controls to operate effectively. Because mitigating controls are 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), in coordination with the Office of the Chief Financial Officer (OCFO) continue the *Financial Systems Modernization* initiative, and make necessary improvements to the Department's financial management systems and supporting IT security controls. Specific recommendations are provided in separate *For Official Use Only* letters provided to DHS management.

Management Comments: We discussed our report with the DHS CFO and CIO and they have agreed with the findings and recommendations reported herein.

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2012 DHS Financial Statement Audit

Below is a description of significant financial management systems and supporting IT infrastructure included in the scope of the DHS FY 2012 financial statement audit.

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 FINCEN in Virginia (VA). The FINCEN is the Coast Guard's primary data center. CAS interfaces with two other systems located at the FINCEN, the Workflow Imaging Network System (WINS) and the Financial and Procurement Desktop (FPD).

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.

Workflow Imaging Network System (WINS)

WINS is the document image processing system, which is integrated with an Oracle Developer/2000 relational database. WINS allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. WINS utilizes MarkView software to scan documents and to view the images of scanned documents and to render images of electronic data received. WINS is interconnected with the CAS and FPD systems and is located at the FINCEN in VA.

Joint Uniform Military Pay System (JUMPS)

JUMPS is a mainframe application used for paying USCG active and reserve payroll. JUMPS is located at the Pay and Personnel Center in Kansas.

Direct Access

Direct Access is the system of record and all functionality, data entry, and processing of payroll events is conducted exclusively in Direct Access. Direct Access is maintained by IBM Application On Demand (IBM AOD) in the iStructure data center facility in Arizona (AZ) with a hot site located in a Qwest data center in VA.

Global Pay (Direct Access II)

Global Pay provides retiree and annuitant support services. Global Pay is maintained by IBM AOD in the iStructure data center facility in AZ with a hot site located in a Qwest data center in VA.

Shore Asset Management (SAM)

SAM is hosted at the Coast Guard's OSC in West Virginia. SAM provides core information about the USCG shore facility assets and facility engineering. The application tracks activities and assist in the management of the Civil Engineering Program and the Facility Engineering Program. SAM data contributes to the shore facility assets full life cycle program management, facility engineering full life cycle program management and rationale to adjust the USCG mission needs through planning, budgeting, and project funding. SAM also provides real property inventory and management of all shore facilities, in addition to the ability to manage and track the facilities engineering equipment and maintenance of that equipment.

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.

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 (AMMIS), 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 hosts the ALMIS application.

CG Treasury Information Executive Repository (CG TIER)

CG TIER is a financial data warehouse containing summarized and consolidated financial data relating USCG operations. It is one of several supporting applications within CAS Suite designed to support the core financial services provided by FINCEN. CG TIER provides monthly submissions to DHS Consolidated TIER.

Integrated Aids to Navigation Information System (IATONIS)

IATONIS is a comprehensive system for managing and reporting on Aids to Navigation and related navigational matters. IATONIS incorporates the Local Notice to Mariners, which is the USCG’s primary means for disseminating information concerning changes to aids to navigation, menaces to navigation, and other timely items of interest to mariners. Additionally, it produces the Light List, the USCG’s official list of all aids to navigation.

Customs and Border Protection (CBP)

Automated Commercial Environment (ACE)

ACE is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. It is CBP’s plan that this system will replace the Automated Commercial System (ACS) when ACE is fully implemented. 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 being deployed in phases, without a final, full deployment date due to funding setbacks. As ACE is partially implemented now and processes a significant amount of revenue for CBP, ACE was included in full scope in the FY 2012 financial statement audit. The ACE system is located in Virginia (VA).

Automated Commercial System (ACS)

ACS is a collection of mainframe-based business process systems used 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, provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations and illegal imports. The ACS system was included in full scope in the FY 2012 financial statement audit. The ACS system is located in VA.

National Data Center – DC Metro Local Area Network (DC Metro LAN)

The DC Metro LAN provides more than 10,000 CBP contractors and employee user's access to enterprise-wide applications and systems. The mission of the DC Metro LAN is to the support the mission of CBP operational elements in the DC Metro LAN region of the organization. These tools include 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. There are 21 major applications supported by the DC Metro LAN, including ACE and ACS. As the DC Metro LAN included the environment where the ACE, ACS, and SAP applications physically reside, the DC Metro LAN was included in the FY 2012 financial statement audit. The DC Metro LAN is located in VA.

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

SAP is a client/server-based financial management system and includes the Funds Management, Budget Control System, General Ledger, Real Estate, Property, Internal Orders, Sales and Distribution, Special Purpose Ledger, and Accounts Payable modules. These modules are used by CBP to manage assets (e.g., budget, logistics, procurement, and related policy), revenue (e.g., accounting and commercial operations: trade, tariff, and law enforcement), and to provide information for strategic decision making. The SAP ECC financial management system was included in full scope in the FY 2012 financial statement audit. The SAP ECC system is located in VA.

Federal Law Enforcement and Training Center (FLETC)

Financial Accounting and Budgeting System (FABS)

The FLETC FABS application 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 I&A/Ops and hosts a separate 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. An application called "Tuxedo," also resides on a separate server. The Tuxedo middleware holds 67 executable files. These files are scripts that process daily information and are not directly accessible by users. The FABS application and servers reside on the FLETC Local Area Network in a Hybrid physical network topology and are accessible from four sites: Georgia (GA), Washington DC, New Mexico, and Maryland.

Glynco Administrative Network

The purpose of the Glynco Administrative Network (GAN) is to provide access to IT network applications and services to include voice 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.

Federal Emergency Management Agency (FEMA)

Integrated Financial Management Information System – Merger (IFMIS-Merger)

IFMIS-Merger is the official accounting system of FEMA and maintains all financial data for internal and external reporting. IFMIS-Merger is comprised of five subsystems: Funding, Cost Posting, Disbursements, Accounts Receivable, and General Ledger. The application is a commercial off-the-shelf software package developed and maintained by Digital Systems Group Incorporated. IFMIS-Merger interfaces with PARS, 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), Fire Grants, eGrants, Enterprise Data Warehouse and Payroll (Department of Agriculture National Finance Center). The IFMIS-Merger production environment is located in Virginia.

Payment and Reporting System (PARS)

PARS is a standalone web-based application. The PARS database resides on the IFMIS-Merger UNIX server and is incorporated within the Certification & Accreditation (C&A) 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-Merger. All payments to grantees are made through IFMIS-Merger. PARS is located in Virginia.

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, submit payments, and view related reports, and by the FEMA 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), 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 Virginia.

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 (PA) (obligation and allocation requests);
- Automated Deployment Database (personnel data);
- Assistance to Firefighters Grants (obligation, invoice and vendor requests);
- Emergency Management Mission Integrated Environment (EMMIE) (obligation requests);
- Mitigation Electronic Grants Management System (obligation requests); and
- CCTMS (expenditure requests).

NDGrants is located in Virginia.

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 PA 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 and IFMIS. EMMIE is located in Virginia.

Traverse

Traverse is the general ledger application currently used by the NFIP Bureau and Statistical Agent to generate the NFIP financial statements. Traverse is a client-server application that runs on the NFIP LAN Windows server environment located in Maryland. 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.

Immigration and Customs Enforcement (ICE)

Federal Financial Management System (FFMS)

The FFMS is a Chief Financial Officer 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 financial reporting system. 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 14 servers are hosted at the DHS DC2 facility located in Virginia. FFMS currently interfaces with Treasury, BMIS Web, and FedTraveler.

ICE Network

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 Mississippi and Virginia. ADEX currently interfaces with the Diplomatic Telecommunications Service Program Office ICENet Infrastructure.

Office of Financial Management (OFM)/Consolidated Component

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 bureaus' core financial management systems. DHSTIER is administered jointly by the OCFO Resource Management Transformation Office (RMTO) and the OCFO Office of Financial Management (OFM) and is hosted on the DHS OneNet at the Stennis Data Center in Mississippi (MS).

Transportation Security Administration (TSA)

Core Accounting System (CAS)

CAS is the core accounting system that records financial transactions and generates financial statements for the United States Coast Guard. CAS is hosted at the Coast Guard's FINCEN in Virginia (VA) and is managed by the United States Coast Guard. The FINCEN is the Coast Guard's primary financial system data center. CAS interfaces with other systems located at the FINCEN, including Financial and Procurement Desktop.

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 hosted at the FINCEN in VA and is and managed by the Coast Guard.

Sunflower

Sunflower is a customized third-party commercial off-the-shelf product used for TSA and Federal Air Marshal Service property management. Sunflower interacts directly with the Office of Finance Fixed Assets module in CAS. Additionally, Sunflower is interconnected to the FPD system and is hosted at the FINCEN in VA and is managed by the Coast Guard.

MarkView

MarkView is imaging and workflow software used to manage invoices in CAS. Each invoice is stored electronically and associated to a business transaction so that users are able to see the image of the invoice. MarkView is interconnected with the CAS system and is located at the FINCEN in VA and is managed by the Coast Guard.

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 / not worked, and provide bi-weekly time records to TSA's payroll provider, the National Finance Center. The system automates the workforce management process to reduce the amount of time, effort, and associated cost required for entry of data.

United States Citizenship and Immigration Services (USCIS)

CLAIMS 3 Local Area Network (LAN)

CLAIMS 3 LAN provides USCIS with a decentralized, geographically dispersed LAN based mission support case management system, with participation in the centralized CLAIMS 3 mainframe data repository. CLAIMS 3 LAN supports the requirements of the Direct Mail Phase I and II, Immigration Act of 1990 (IMMACT 90) and USCIS forms improvement projects. The CLAIMS 3 LAN is located at the following service centers and district offices: Nebraska, California, Texas, Vermont, Baltimore District Office, National Business Center, and Administrative Appeals Office. CLAIMS 3 LAN interfaces with the following systems:

- Citizenship and Immigration Services Centralized Oracle Repository
- CLAIMS 3 Mainframe
- Integrated Card Production System
- CLAIMS 4
- E-filing
- Benefits Biometric Support System
- Refugee, Asylum, and Parole System
- National File Tracking System
- Integrated Card Production System
- Customer Relationship Interface System
- USCIS Enterprise Service Bus

CLAIMS 4

The purpose of CLAIMS 4 is to track and manage naturalization applications. Claims 4 is a client/server application. The central Oracle Database is located in Washington, DC while application servers and client components are located throughout USCIS service centers and district offices. CLAIMS 4 interfaces with the following systems:

- Central Index System (CIS)
- Reengineered Naturalization Automated Casework System
- CLAIMS 3 LAN and Mainframe
- Refugee, Asylum, and Parole System
- Enterprise Performance Analysis System
- National File Tracking System
- Asylum Pre-Screening System
- USCIS Enterprise Service Bus
- Biometrics Benefits Support System
- Enterprise Citizenship and Immigration Service Centralized Operational Repository
- Customer Relationship Interface System
- FD 258 Enterprise Edition and Mainframe
- Site Profile System

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 financial reporting system. 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 14 servers are hosted at the DHS DC2 facility located in Virginia. FFMS currently interfaces with Treasury, BMIS Web, and FedTraveler.

CIS1 Network

The USCIS network, also known as 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 Virginia and Nebraska.

Appendix B

FY 2012 Notices of IT Findings and Recommendations at DHS

United States Coast Guard

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-12-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process	Access Controls		X
CG-IT-12-02	Civilian Background Investigations	Security Management		X
CG-IT-12-03	Contractor Background Investigations	Security Management		X
CG-IT-12-04	Inappropriate Access to JUMPS SMF Audit Logs	Access Controls	X	
CG-IT-12-05	Direct Access & Direct Access II Audit Logging	Access Controls		X
CG-IT-12-06	OSC Data Center Visitor Access Logs	Access Controls		X
CG-IT-12-07	Physical Configuration Audits of NESSS System Changes	Configuration Management	X	
CG-IT-12-08	Direct Access and Direct Access II PeopleSoft System Administrator and Security Administrator Accounts	Access Controls	X	
CG-IT-12-09	Security Awareness Issues Identified During Social Engineering Testing at Surface Forces Logistics Center	Access Controls		X
CG-IT-12-10	Security Awareness Issues Associated with Physical Protection of Sensitive Information	Access Controls		X
CG-IT-12-11	Weaknesses related to IA Professionals’ Required Certifications	Security Management		X
CG-IT-12-12	Naval & Electronics Supply System User Access	Access Controls		X
CG-IT-12-13	AMMIS Software Change Requests Process	Configuration Management		X
CG-IT-12-14	Configuration Management Controls over the Scripting Process	Configuration Management		X
CG-IT-12-15	Direct Access User Account Recertification	Access Controls		X
CG-IT-12-16	Access and Configuration Management Controls – Vulnerability Assessment	Configuration Management		X
CG-IT-12-17	IATONIS Audit Log Review	Access Controls	X	
CG-IT-12-18	IATONIS Separation of Duties	Segregation of Duties	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-12-19	Functional Configuration Audits of IATONIS System Changes	Configuration Management	X	
CG-IT-12-21	NESSS User Recertification	Access Controls		X
CG-IT-12-22	IATONIS Account Recertification	Access Controls	X	

Customs and Border Protection

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-12-01	Physical Security Issues Identified During Enhanced Security Testing	Access Controls		X
CBP-IT-12-02	Inadequate Role-Based Security Training Program	Security Management		X
CBP-IT-12-03	Segregation of Duties Control Weaknesses within CBP System	Access Controls		X
CBP-IT-12-04	CBP System User Profile Change Logs are not Reviewed	Access Controls		X
CBP-IT-12-05	CBP System User Profile Change Logs are not Reviewed	Access Controls		X
CBP-IT-12-06	Weaknesses in Creating New CBP System Accounts	Access Controls		X
CBP-IT-12-07	CBP System Audit Logs not Appropriately Reviewed	Access Controls		X
CBP-IT-12-08	Incomplete Background Re-Investigations for CBP Employees and Contractors	Security Management		X
CBP-IT-12-09	Contractor NDAs are Incomplete	Security Management		X
CBP-IT-12-10	Lack of Annual Recertification for CBP System Application Users	Access Controls	X	
CBP-IT-12-11	Incomplete Documentation of ISAs for CBP System Connections	Access Controls	X	
CBP-IT-12-12	Inadequate Documentation for CBP System Application Software Changes	Configuration Management	X	
CBP-IT-12-13	CBP System DB2 Database Patches are not Documented and Implemented Appropriately	Configuration Management	X	
CBP-IT-12-14	CBP System AIX Operating System Patches are not Implemented Appropriately	Configuration Management	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-12-15	CBP System Production and Training Operating Systems Vulnerability Scanning Process Weaknesses and Scan Results	Configuration Management		X
CBP-IT-12-16	Lack of Access Requests and Approvals for CBP System Accounts	Access Controls		X
CBP-IT-12-17	Lack of Monitoring Developer Emergency/Temporary Access to CBP System Production	Access Controls		X
CBP-IT-12-18	Lack of Annual Recertification for CBP System Privileged Users	Access Controls	X	
CBP-IT-12-19	Incomplete Documentation of ISAs for CBP System Connections	Access Controls		X
CBP-IT-12-20	Inadequate Documentation for CBP System Application Software Changes	Configuration Management	X	
CBP-IT-12-21	CBP System LPARs and Linux z/OS Vulnerability Scanning Process Weaknesses and Scan Results	Configuration Management	X	
CBP-IT-12-22	CBP System Raised Floor Access Weaknesses	Access Controls	X	
CBP-IT-12-23	Lack of Functionality in the CBP System	Application Controls		X
CBP-IT-12-24	Inadequate Documentation of CBP System Access Requests	Access Controls		X
CBP-IT-12-25	Incomplete Access Request Approval Forms for New Remote Access User Account	Access Controls		X
CBP-IT-12-26	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-27	Separated Personnel on CBP System User Listing	Access Controls	X	
CBP-IT-12-28	Lack of Annual Recertification for CBP System Application, Oracle Database and Operating System Account Recertifications	Access Controls	X	
CBP-IT-12-29	CBP System Audit Logs are not Appropriately Reviewed	Access Controls	X	
CBP-IT-12-30	CBP System Technical Vulnerability Weaknesses	Configuration Management	X	
CBP-IT-12-31	Lack of Complete Review of CBP System Profile Changes	Access Controls	X	
CBP-IT-12-32	CBP System Vulnerability Scanning Process Weaknesses and Scan Results	Configuration Management	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CBP-IT-12-33	CBP System Configuration Setting for Disabling Inactive Accounts is not Configured Appropriately	Access Controls	X	
CBP-IT-12-34	Incomplete Documentation of ISAs for CBP System Connections	Access Controls	X	
CBP-IT-12-36	CBP System Oracle Database and Unix Operating Systems Patches are not Documented and Implemented Appropriately	Configuration Management	X	
CBP-IT-12-38	Employee Separation Process Weaknesses	Security Management		X
CBP-IT-12-39	Contractor Separation Process Weaknesses	Security Management		X
CBP-IT-12-40	CBP System Segregation of Duties Weaknesses over the Production Environment	Configuration Management		X
CBP-IT-12-41	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-42	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-43	CBP System Security Authorization Documentation is Not Documented, Approved, and Kept Up-To Date.	Access Controls	X	
CBP-IT-12-45	CBP System Program Library Access not Documented and Approved Appropriately.	Configuration Management	X	
CBP-IT-12-46	Separated Personnel on CBP System User Listing	Access Controls	X	
CBP-IT-12-47	Separated Personnel on CBP System User Listing	Access Controls		X
CBP-IT-12-48	Separated Personnel on CBP System Application and Operating System User Listing	Access Controls		X
CBP-IT-12-49	CBP System Audit Log Review Weaknesses	Access Controls	X	

Federal Emergency Management Agency

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-12-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-12-02	All Required Auditable Events Not Included in Traverse Audit Logs	Access Controls		X
FEMA-IT-12-03	Inadequate Retention of NFIP LAN Audit Logs	Access Controls		X
FEMA-IT-12-04	Inadequate Documentation Supporting IFMIS-Merger User Functions	Access Controls		X
FEMA-IT-12-05	Incomplete Recertification of Traverse Application User Privileges	Access Controls	X	
FEMA-IT-12-06	Weaknesses Identified during the Vulnerability Assessment on IFMIS	Access Controls and Configuration Management		X
FEMA-IT-12-07	Weaknesses Identified during the Vulnerability Assessment on the NFIP LAN	Access Controls and Configuration Management	X	
FEMA-IT-12-08	Weaknesses Identified during the Vulnerability Assessment on Financially Significant Segments of the FEN and End-User Computing Environment	Access Controls and Configuration Management	X	
FEMA-IT-12-09	Weaknesses Identified during the Vulnerability Assessment on EMMIE	Access Controls and Configuration Management	X	
FEMA-IT-12-10	Weaknesses Identified during the Vulnerability Assessment on NDGrants	Access Controls and Configuration Management	X	
FEMA-IT-12-11	Inconsistent Authorization of New and Modified IFMIS-Merger Application User Access	Access Controls	X	
FEMA-IT-12-12	Untimely Removal of FEN Access Privileges for Separated FEMA Employees	Access Controls		X
FEMA-IT-12-13	Incomplete Implementation of Role-Based Training for Individuals with Significant Information Security Responsibilities	Security Management		X
FEMA-IT-12-14	Incomplete POA&Ms for Internal NFIP LAN Vulnerability Assessments	Configuration Management	X	
FEMA-IT-12-15	Weaknesses in the Management of POA&Ms for Audit Findings over FEMA Financial Systems	Security Management		X

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-12-16	Inconsistent Review of Audit Logs of IFMIS-Merger System Software Administrator Activity	Access Controls	X	
FEMA-IT-12-17	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems	Configuration Management		X
FEMA-IT-12-18	Non-Compliance with DHS Policy for Approval of Shared Accounts on the FEN	Access Controls	X	
FEMA-IT-12-19	Non-Compliance with DHS Policy for Approval of Remote Access to the FEN	Access Controls	X	
FEMA-IT-12-20	Lack of ISA between FEMA and Department of Justice	Access Controls	X	
FEMA-IT-12-21	Inadequate Security Authorization Documentation for the FEN	Security Management		X
FEMA-IT-12-22	Lack of CMP Documentation for ES	Configuration Management	X	
FEMA-IT-12-23	Lack of Testing Traverse Application Changes Prior to Implementation	Configuration Management		X
FEMA-IT-12-24	Inconsistent Documentation of TRRP Configuration Changes	Configuration Management		X
FEMA-IT-12-25	Inconsistent Review of PARS Database Audit Logs	Access Controls	X	
FEMA-IT-12-26	Lack of BIA Supporting the NDGrants CP	Contingency Planning	X	
FEMA-IT-12-27	Lack of Alternate Processing Site and Sufficient CP Testing for NDGrants	Contingency Planning	X	
FEMA-IT-12-28	Inconsistent Implementation of DHS Background Investigation Requirements for FEMA Federal Employees and Contractors	Security Management		X
FEMA-IT-12-29	Non-Compliance with DHS Policies for IFMIS-Merger Security Authorization Documentation	Security Management	X	
FEMA-IT-12-30	Lack of Adequate IFMIS-Merger CP and Plan Test Documentation	Contingency Planning	X	
FEMA-IT-12-31	Approval of Elevated Privileges Was Not Consistent with DHS Policy	Access Controls	X	
FEMA-IT-12-32	Lack of EMMIE System Owner Approval for Database Accounts	Access Controls	X	
FEMA-IT-12-33	Incomplete Access Procedures for Operations Branch Database Accounts	Access Controls	X	
FEMA-IT-12-34	Lack of ES System Owner Approval for Database Accounts	Access Controls	X	
FEMA-IT-12-35	Lack of NDGrants System Owner Approval for Database Accounts	Access Controls	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-12-36	Inconsistent Review of IFMIS-Merger Application and Database Audit Logs	Access Controls		X
FEMA-IT-12-37	Insufficient Development and Update of the EMMIE CP	Contingency Planning	X	
FEMA-IT-12-38	Non-Compliance with Alternate Processing Site Requirements for EMMIE	Contingency Planning	X	
FEMA-IT-12-39	Insufficient Review and Approval of the ES CP	Contingency Planning	X	
FEMA-IT-12-40	Non-Compliance with Alternate Processing Site Requirements for ES	Contingency Planning	X	
FEMA-IT-12-41	Incomplete POA&Ms for EMMIE SAR Weaknesses	Security Management	X	
FEMA-IT-12-42	Non-Compliant Security Authorization Package for NDGrants	Security Management	X	
FEMA-IT-12-43	Non-Compliant Security Authorization Package for ES	Security Management	X	
FEMA-IT-12-44	Incomplete Account Management Procedures for the EMMIE Application	Access Controls	X	
FEMA-IT-12-45	Incomplete Account Management Procedures for NDGrants	Access Controls	X	
FEMA-IT-12-46	Incomplete Account Management Procedures for ES	Access Controls	X	
FEMA-IT-12-47	Non-Compliance with DHS and FEMA Password Requirements for Oracle Databases Supporting Financial Applications	Access Controls	X	
FEMA-IT-12-48	Incomplete Waiver Request for Password Controls on Oracle Databases Supporting Financial Applications	Access Controls	X	
FEMA-IT-12-49	Inconsistent Authorization of Temporary Access to IFMIS-Merger System Software	Access Controls and Configuration Management		X
FEMA-IT-12-50	Inadequate Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment	Configuration Management		X
FEMA-IT-12-51	Inconsistent Activities and Incomplete Documentation Supporting Configuration Changes for the IFMIS-Merger Application	Configuration Management	X	
FEMA-IT-12-52	Lack of ES Information System Security Officer Review of Monthly Vulnerability Scan Results	Configuration Management	X	
FEMA-IT-12-53	Insufficient Audit Log Controls for EMMIE	Access Controls	X	
FEMA-IT-12-54	Insufficient Audit Log Controls for NDGrants	Access Controls	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-12-55	Insufficient Audit Log Controls for ES	Access Controls	X	
FEMA-IT-12-56	Incomplete Documentation Supporting EMMIE Configuration Management Controls	Configuration Management	X	
FEMA-IT-12-57	Unauthorized Shared Account Usage for EMMIE and NDGrants Production Application Deployments	Configuration Management	X	
FEMA-IT-12-58	Lack of Controls to Validate Completeness and Integrity of EMMIE and NDGrants Application Changes Deployed to Production	Configuration Management	X	
FEMA-IT-12-59	Incomplete Documentation Supporting NDGrants Configuration Management Controls	Configuration Management	X	
FEMA-IT-12-60	Incomplete Vulnerability Management Procedures	Configuration Management	X	
FEMA-IT-12-61	Excessive or Inappropriate Access to IFMIS	Access Controls	X	

Federal Law Enforcement Training Center

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-12-01	Ineffective Segregation of Duties Controls for the Momentum System	Segregation of Duties		X
FLETC-IT-12-02	FLETC Servers and Workstations have Inadequate Patch Management	Configuration Management	X	
MGA-IT-12-03	I&A/Ops Momentum Access Controls are not Consistently Applied	Access Controls	X	
MGA-IT-12-04	Configuration Changes for the I&A/Ops Momentum System are not Consistently Documented	Configuration Management	X	

Immigration and Customs Enforcement

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-12-01	FFMS Network and Servers were Installed with Default Configuration Settings and Protocols	Configuration Management		X
ICE-IT-12-02	FFMS Mainframe Production Databases were Installed and Configured without Baseline Security Configurations	Configuration Management		X
ICE-IT-12-03	FFMS Servers have Inadequate Patch Management	Configuration Management		X
ICE-IT-12-04	FFMS Access Recertification Reviews are Not Completed	Access Controls		X
ICE-IT-12-05	Weak FFMA Segregation of Duties	Segregation of Duties		X
ICE-IT-12-06	Security Awareness Issues Identified During After-Hours Walkthrough	Security Management		X
ICE-IT-12-07	Lack of Procedures for Transferred/Terminated Personnel Exit Processing	Access Controls		X
ICE-IT-12-08	ICE Servers and Workstation have Inadequate Patch Management	Access Controls		X
ICE-IT-12-09	ICE Servers and Workstations were Installed with Default Configuration Settings and Protocols	Configuration Management	X	
ICE-IT-12-10	Lack of Recertification for ADEX Users	Access Control	X	
ICE-IT-12-11	Inadequate FFMS User Access Request Forms	Access Control	X	

National Protection and Programs Directorate

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
NPPD-IT-12-01	Security Awareness Issues Identified During After-Hours Walkthrough	Security Management	X	
NPPD-IT-12-02	Security Awareness Issues were identified during Social Engineering	Security Management	X	

Office of Financial Management / Office of Chief Information Officer

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-12-01	Network Logical Access Parameters are not Configured in Accordance with DHS Policy	Access Controls		X
CONS-IT-12-02	TIER Configuration Management procedures not consistently executed	Configuration Management	X	
CONS-IT-12-03	Security Awareness Issues Identified During After-Hours Walkthrough	Security Management		X
OCIO-IT-12-01	DHS has not Fully Implemented the Federal Desktop Core Configuration (FDCC) Security Configurations Requirements	Security Management		X
OCIO-IT-12-02	DHS Physical Controls could be Strengthened	Access Controls		X
OCIO-IT-12-03	DHS Infrastructure Configuration Management procedures not adequately defined	Configuration Management	X	
OCIO-IT-12-04	Ineffective safeguards over physical access to sensitive facilities and resources	Access Controls	X	

Transportation Security Administration

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-12-01	Physical Security and Security Awareness Issues identified during enhanced security testing	Access Controls		X
TSA-IT-12-02	Computer Access Agreements	Access Controls		X
TSA-IT-12-03	eTAS User Account Recertification	Access Controls	X	
TSA-IT-12-04	eTAS User Passwords	Access Controls	X	
TSA-IT-12-05	eTAS Restoration Testing of Media Backups	Contingency Planning	X	
TSA-IT-12-06	eTAS Audit Logs	Access Controls	X	
TSA-IT-12-07	eTAS System User Access	Access Controls	X	
TSA-IT-12-08	Configuration Management Controls Over the Coast Guard Scripting Process	Configuration Management		X

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
TSA-IT-12-09	eTAS Pre-Implementation Deficiencies	Security Management	X	

United States Citizenship and Immigration Services

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-12-01	Policies and Procedures for CLAIMS 3 LAN and CLAIMS 4 Audit Logs	Access Controls		X
CIS-IT-12-02	Inadequate Access Request Forms for CLAIMS 4 System Users	Access Controls		X
CIS-IT-12-03	Weak Logical Access Controls exist over CLAIMS 4	Access Controls		X
CIS-IT-12-04	Security Awareness Issues Identified during After-Hours Walkthrough	Security Management	X	
CIS-IT-12-05	Lack of Segregation of Duties for CLAIMS 3 LAN	Access Controls		X
CIS-IT-12-06	Periodic User Access Reviews are not Performed for CLAIMS 3 LAN Users	Access Controls		X
CIS-IT-12-07	FFMS Vulnerability Weaknesses Impact USCIS Operations	Configuration Management		X
CIS-IT-12-08	Security Awareness Issues were Identified during Social Engineering	Security Management	X	
CIS-IT-12-09	Procedures for Transferred/Terminated Personnel Exit Processing are not Finalized	Access Controls		X
CIS-IT-12-10	Lack of Policies and Procedures for Separated CLAIMS 3 LAN Accounts	Access Controls		X
CIS-IT-12-11	Equipment and Media Policies and Procedures are not Current	Access Controls		X
CIS-IT-12-12	Lack of Computer Security Awareness Training Compliance	Security Management		X
CIS-IT-12-13	Lack Role-Based Training for Key Security Personnel	Security Management		X
CIS-IT-12-14	Lack of ATO for CLAIMS 3 LAN	Security Management	X	
CIS-IT-12-15	Lack of ATO for CLAIMS 4	Security Management	X	
CIS-IT-12-16	Lack of Segregation of Duties Controls Exist over CIS 1	Segregation of Duties	X	

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-12-17	Visitor Access Controls are Inadequate at the VSC	Access Controls	X	
CIS-IT-12-18	Inadequate CIS1 Access Request Forms for Temporary Users	Access Controls	X	
CIS-IT-12-19	Incomplete Recertification for CIS 1 Network Administrators	Access Controls	X	

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at DHS

Customs and Border Protection

NFR #	Description	Disposition	
		Closed	Repeat
CBP-IT-11-01	Security Awareness Issued Identified During Enhanced Security Testing	X	
CBP-IT-11-02	Physical Security Issues Identified during Enhanced Security Testing		X
CBP-IT-11-03	Inadequate Role-based Security Training Program		X
CBP-IT-11-04	Segregation of Duties Control Weaknesses within the CBP System		X
CBP-IT-11-05	CBP System User Access Profile Change Log Review Procedures Have Not Been Implemented		X
CBP-IT-11-07	Lack of Monitoring of Developer Emergency/Temporary Access to CBP System Production		X
CBP-IT-11-08	Lack of Monitoring of CBP System Novell Server Audit Logs	X	
CBP-IT-11-09	Lack of Update to CBP System Contingency Plan	X	
CBP-IT-11-10	Lack of Update to CBP System Security Plan	X	
CBP-IT-11-11	Background Investigations and Reinvestigations for CBP Employees and Contractors are not Completed		X
CBP-IT-11-12	Contractor Separation procedures are not Updated and Contractor Separation forms are not Maintained		X
CBP-IT-11-13	Lack of Access Requests and Approval for CBP System Accounts		X
CBP-IT-11-14	CBP System Profile Change Logs are not Reviewed		X
CBP-IT-11-15	CBP System User Access Form Documentation is Incomplete		X
CBP-IT-11-16	CBP System Privileged User Recertification is Incomplete	X	
CBP-IT-11-17	Remote User Access Form Documentation is Incomplete		X
CBP-IT-11-18	CBP System Interconnection Security Agreements are Incomplete		X
CBP-IT-11-19	Contractor Non-Disclosure Agreement Weaknesses		X
CBP-IT-11-20	Employee Separations Weaknesses		X
CBP-IT-11-21	CBP System Audit Log Review Weaknesses		X

NFR #	Description	Disposition	
		Closed	**Repeat**
CBP-IT-11-22	CBP System User Access Authorization Evidence Weakness		X
CBP-IT-11-23	CBP System Security Test & Evaluation Weakness	X	
CBP-IT-11-24	CBP System Configuration Management Policies and Procedures not Finalized	X	
CBP-IT-11-25	CBP System Account Authentication Weaknesses	X	
CBP-IT-11-26	CBP System Audit Log Review Weaknesses	X	
CBP-IT-11-27	Security Weaknesses Identified during Technical Vulnerability Assessment		X
CBP-IT-11-28	Security Posture of CBP Workstations	X	
CBP-IT-11-30	Separated Personnel on CBP System User Listings		X
CBP-IT-11-31	CBP System Functionality Issues		X
CBP-IT-11-32	CBP System User Account Termination Weaknesses		X
CBP-IT-11-33	CBP System Security Test & Evaluation Weakness	X	
CBP-IT-11-34	CBP System Security Test & Evaluation Weakness	X	
CBP-IT-11-35	Evidence of Personnel Authorization to Access Backup Media Not Available	X	
CBP-IT-11-36	CBP System Recertification Weaknesses	X	
CBP-IT-11-37	CBP System Privileged User Access Management Process Weaknesses	X	
CBP-IT-11-38	CBP System Privileged User Segregation of Duties Weaknesses		X

Note 1: NFRs numbers CBP-IT-11-06 and CBP-IT-11-29 were not used in the FY 2011 IT NFR sequence.

Note 2: Specific system names were replaced with “CBP System” for security purposes.

United States Coast Guard

NFR #	Description	Disposition	
		Closed	**Repeat**
CG-IT-11-01	Security Awareness Issues Associated with Physical Protection of Sensitive Information		X
CG-IT-11-02	Direct Access and Direct Access II User and System Administrator Account Management and Approval	X	
CG-IT-11-03	CG-TIER resource owners' identification of authorized users	X	
CG-IT-11-04	Weaknesses Related to IA Professionals' Required Certifications		X
CG-IT-11-05	Configuration Management Controls over the Scripting Process		X
CG-IT-11-06	Civilian Background Investigations		X
CG-IT-11-07	Contractor Background Investigations		X
CG-IT-11-08	Security Awareness Issues Associated with the Social Engineering Testing		X
CG-IT-11-09	OSC Data Center Visitor Access Logs		X
CG-IT-11-10	Direct Access and Direct Access II Audit Logging and General IT Control Validation		X
CG-IT-11-11	AMMIS Software Change Requests Process		X
CG-IT-11-12	SAM and NESSS Audit Log Review	X	
CG-IT-11-13	Direct Access System User Account Recertification		X
CG-IT-11-14	NESSS Access Authorizations		X
CG-IT-11-15	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems		X
CG-IT-11-16	Naval & Electronics Supply Support System Users Who Have Admin Capabilities	X	
CG-IT-11-17	ALMIS User Recertification	X	
CG-IT-11-18	Non-Compliance with FFMIA – Information Technology	X	
CG-IT-11-19	Weaknesses Associated with the Coast Guard Security Incident Database and Ticket System	X	
CG-IT-11-20	Access and Configuration Management Controls – Vulnerability Assessment		X

NFR #	Description	Disposition	
		Closed	Repeat
CG-IT-11-21	Naval and Electronics Supply Support System User Account Recertification		X

United States Citizenship and Immigration Services

NFR #	Description	Disposition	
		Closed	Repeat
CIS-IT-11-01	Equipment and media policies and procedures are not current		X
CIS-IT-11-02	Weak password configuration controls for CLAIMS 4	X	
CIS-IT-11-03	Policies and procedures for CLAIMS 3 LAN and CLAIMS 4 audit logs		X
CIS-IT-11-04	Policies and procedures for separated CLAIMS 3 LAN accounts		X
CIS-IT-11-05	Periodic user access reviews are not performed for CLAIMS 3 LAN users		X
CIS-IT-11-06	Procedures for transferred/terminated personnel exit processing are not finalized		X
CIS-IT-11-07	Incomplete or inadequate access request forms for CLAIMS 3 LAN and CLAIMS 4 system users		X
CIS-IT-11-08	ICE resource server and inadequate patch management weaknesses impact USCIS operations	X	
CIS-IT-11-09	Weak password configuration controls for CLAIMS 3 LAN	X	
CIS-IT-11-10	Weak logical access controls exist over CLAIMS 4		X
CIS-IT-11-11	Ineffective safeguards over physical access to sensitive facilities and resources	X	
CIS-IT-11-12	VPN access request forms are not properly maintained	X	
CIS-IT-11-13	Lack of Segregation of Duties for CLAIMS 3 LAN		X
CIS-IT-11-14	ADEX access request forms are not properly maintained	X	
CIS-IT-11-15	Lack of Computer Security Awareness Training Compliance		X
CIS-IT-11-16	Lack role-based training for key security personnel		X
CIS-IT-11-17	FFMS Vulnerability Weaknesses effect USCIS Operations		X

Office of Financial Management / Office of Chief Information Officer

NFR #	Description	Disposition	
		Closed	Repeat
CONS-IT-11-01	Network Logical Access Parameters are not Configured in Accordance with DHS policy		X
CONS-IT-11-02	Security Awareness issues identified during After-Hours Walkthrough		X
OCIO-IT-11-01	DHS has not Fully Implemented the Federal Desktop Core Configuration (FDCC) Security Configurations Requirements		X
OCIO-IT-11-02	DHS physical controls could be strengthened		X

Federal Emergency Management Agency

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-01	Alternate Processing Site for NEMIS Has Not Been Established	X	
FEMA-IT-11-02	Weaknesses Exist in the C&A Package for the FEMA Switched Network (FSN)-2, which Includes the FEMA LAN		X
FEMA-IT-11-03	Weaknesses Exist over the ATO and C&A Documentation for NEMIS	X	
FEMA-IT-11-04	NEMIS CP Does Not Comprehensively Address the Requirements of DHS Policy and Has Not Been Adequately Tested	X	
FEMA-IT-11-05	Formalized Training Requirements for Individuals with Significant Information Security Responsibilities Have Not Been Fully Implemented and Role-Based Training is Not Tracked or Monitored		X
FEMA-IT-11-06	Documentation Supporting IFMIS-Merger User Functions Does Not Exist		X
FEMA-IT-11-07	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary are Not Configured to Enforce Password Requirements	X	
FEMA-IT-11-08	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary Do Not Adequately Enforce Account Lockout Requirements	X	

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-09	Operating System Audit Logging on Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate	X	
FEMA-IT-11-10	Weaknesses Existed over Contingency Planning, Testing and Development of the Continuity of Operations Plan for TRRP and Traverse	X	
FEMA-IT-11-11	Recertification of NEMIS Access Control System Position Assignments is Incomplete	X	
FEMA-IT-11-12	Audit Logging on Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate	X	
FEMA-IT-11-13	Weaknesses Exist over Vulnerability Management for Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary	X	
FEMA-IT-11-14	NFIP Physical Access Policies and Procedures were Not Appropriately Documented and Implemented	X	
FEMA-IT-11-15	NFIP LAN and Traverse Account Security Configuration Is Not in Compliance with DHS Policy	X	
FEMA-IT-11-16	TRRP Logical Access was Not Appropriately Authorized	X	
FEMA-IT-11-17	Weaknesses Exist over Configuration and Operating Effectiveness of Traverse Audit Logs		X
FEMA-IT-11-18	Inadequate Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment		X
FEMA-IT-11-19	Weaknesses Exist over Configuration Management Processes for Financial Applications within the Previous NEMIS Accreditation Boundary	X	
FEMA-IT-11-20	Weaknesses Exist over IFMIS-Merger Configuration Management Processes	X	
FEMA-IT-11-21	Weaknesses Exist over Recertification of Access to the IFMIS-Merger Application	X	
FEMA-IT-11-22	Weaknesses Exist over TRRP Mainframe Audit Logs	X	
FEMA-IT-11-23	Emergency and Temporary Access to IFMIS-Merger is Not Properly Authorized		X
FEMA-IT-11-24	Weaknesses Exist over IFMIS-Merger Application and Database Audit Logging		X
FEMA-IT-11-25	IFMIS–Merger User Access was Not Managed in Accordance with Account Management Procedures	X	
FEMA-IT-11-26	PARS Database Security Controls Are Not Appropriately Established	X	
FEMA-IT-11-27	NFIP LAN Audit Logging is Not Performed in Accordance with DHS and FEMA Requirements		X

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-28	Individual User Virtual Private Network (VPN) Access Accounts are Not Appropriately Authorized or Recertified	X	
FEMA-IT-11-29	External Connections to the FEMA VPN Are Not Appropriately Authorized or Documented	X	
FEMA-IT-11-30	IFMIS-Merger System Software Administrator Activity Is Not Appropriately Restricted or Monitored	X	
FEMA-IT-11-31	Weaknesses Exist over C&A Documentation for IFMIS-Merger	X	
FEMA-IT-11-32	Risk Assessment Activities over NFIP IT Systems were Not Adequately Performed	X	
FEMA-IT-11-33	Weaknesses Exist over Management and Technical Controls Associated with FEMA LAN Accounts		X
FEMA-IT-11-34	Employee Termination Process for Removing System Access Should Be More Proactive	X	
FEMA-IT-11-35	Traverse Configuration Management Plan Weaknesses		X
FEMA-IT-11-36	TRRP Configuration Management Plan Weaknesses		X
FEMA-IT-11-37	Documentation Supporting TRRP Test Libraries Does Not Reflect Current Environment	X	
FEMA-IT-11-38	Federal Insurance and Mitigation Administration CMP has Not Been Developed	X	
FEMA-IT-11-39	Weaknesses Exist over Background Investigations for Federal Employees and Contractors		X
FEMA-IT-11-40	Weaknesses in the Management of POA&Ms for Audit Findings over FEMA Financial Systems		X
FEMA-IT-11-41	Physical Security and Security Awareness Issues Associated with Enhanced Security Testing at FEMA		X
FEMA-IT-11-42	Traverse Accounts Were Not Appropriately Recertified	X	
FEMA-IT-11-43	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems		X
FEMA-IT-11-44	Password, Patch, and Configuration Management Weaknesses Were Identified during the Vulnerability Assessment on IFMIS, NEMIS, and Key Support Servers		X
FEMA-IT-11-45	Vulnerability Assessment Program for the NFIP LAN Supporting Traverse was Inadequate	X	
FEMA-IT-11-46	Weaknesses Existed over the Configuration Patch Management Process for the NFIP LAN Supporting Traverse	X	
FEMA-IT-11-47	Weaknesses Exist over the Configuration and Testing of Backups for Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary	X	

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-48	Key Controls over Production Servers Supporting Applications within the Former NEMIS Accreditation Boundary Have Not Been Implemented	X	

Federal Law Enforcement Training Center

NFR #	Description	Disposition	
		Closed	Repeat
FLETC-IT-11-01	Ineffective Logical Access Controls over the GAN	X	
FLETC-IT-11-02	Ineffective Segregation of Duties controls for the Momentum System		X

Immigration and Customs Enforcement

NFR #	Description	Disposition	
		Closed	Repeat
ICE-IT-11-01	ADEX Resource Servers and Workstations have Inadequate Patch Management		X
ICE-IT-11-02	Terminated/Transferred Personnel are not Removed from ADEX in a Timely Manner	X	
ICE-IT-11-03	Access Recertification Review is not completed for FFMS		X
ICE-IT-11-04	Weak FFMS Segregation of Duties		X
ICE-IT-11-05	Security Awareness issues were identified during Social Engineering	X	
ICE-IT-11-06	FFMS Network and Servers were installed with Default Configuration Settings and Protocols		X
ICE-IT-11-07	FFMS Mainframe Production databases were installed and configured without baseline security configurations		X
ICE-IT-11-08	FFMS servers have inadequate patch management		X
ICE-IT-11-09	Default installation and configuration of Cisco routers on ICE Network	X	
ICE-IT-11-10	Security Awareness issues identified during After-Hours Walkthrough		X

NFR #	Description	Disposition	
		Closed	**Repeat**
ICE-IT-11-11	Lack of procedures for transferred/terminated personnel exit processing		X

Transportation Security Administration

NFR No.	Description	Disposition	
		Closed	**Repeat**
TSA-IT-11-01	Markview – Password Settings	X	
TSA-IT-11-02	Markview – Administrator Account	X	
TSA-IT-11-03	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		X
TSA-IT-11-04	TSA Computer Access Agreement Process		X
TSA-IT-11-05	Sunflower and Markview User Account Recertifications	X	
TSA-IT-11-06	Configuration Management Controls Over the Coast Guard Scripting Process		X

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.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: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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