Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for FY 2011 Department of Homeland Security Financial Statement Audit

OIG-12-81

May 2012

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

May 3, 2012

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This report presents the information technology (IT) management letter for the DHS financial statement audit as of September 30, 2011. It contains observations and recommendations related to information technology internal control weaknesses that were summarized in the *Independent Auditors Report* dated November 11, 2011, and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of the DHS' FY 2011 financial statement audit and prepared this IT management letter. KPMG is responsible for the attached IT management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

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

March 27, 2012

Acting Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Department of Homeland Security

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, 2011 and the related statement of custodial activity for the year then ended (referred to herein as the "fiscal year (FY) 2011 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 balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended. In connection with our audit, we also considered DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the FY 2011 financial statements.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 11, 2011, included internal control deficiencies identified during our audit, that individually, or in aggregate, represented a material weakness or a significant deficiency. This letter represents the separate limited distribution report mentioned in that report.

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to DHS' financial systems general Information Technology (IT) controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. 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.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also 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), and are intended For Official Use Only. 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 2011 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 and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General (OIG), U.S. Office of Management and Budget (OMB), U.S. Government Accountability Office (GAO), and the U.S. Congress, 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 IT general controls 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 IT general controls 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 general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the general IT controls 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 general IT controls audit procedures, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls in the DHS environment. 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 key general support systems.

In addition, we performed application control tests on a limited number of DHS' financial systems and applications. The application control testing was performed to assess the input, processing, and output of financial data and transactions that support the financial systems' internal controls. Application controls are 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 a separate *Limited Official Use* IT Management letter provided to component management and the OIG.

In recent years, we've 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 eight years ago. Therefore, in FY 2011, we continued to evaluate and consider the impact of financial system functionality over financial reporting.

SUMMARY OF FINDINGS AND RECOMMENDATION

During our FY 2011 assessment of IT general and application controls and financial system functionality, we noted that the DHS made some progress in remediation of IT findings we reported in FY 2010. We have closed approximately 30 percent of our prior year IT findings. The Immigration and Customs Enforcement (ICE), Federal Emergency Management Agency (FEMA), and Federal Law Enforcement Training Center (FLETC) made the most progress in closing IT findings from the prior year. In addition, we issued fewer new findings in FY 2011 compared to the number of new findings in FY 2010. In FY 2011, we identified approximately 147 findings, of which approximately 72 percent are repeated from last year. Approximately 44 percent of our repeat findings were for IT deficiencies that management represented were corrected during FY 2011. The majority of new deficiencies were noted at Customs Border and Protection (CBP).

The most significant weaknesses from a financial statement audit perspective 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 compliance; 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 Systems Functionality for the FY 2011 audit of the DHS consolidated financial statements.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATION

In FY 2011, a number of IT and financial system functionality deficiencies were identified at DHS. Approximately 147 findings were identified of which approximately 72 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.

Conditions: Our findings related to general IT controls and financial systems functionality follow:

Related to IT controls:

1. *Access controls*:
    - Deficiencies in management of application and/or database accounts, network, and remote user accounts.
        - System administrator root access to financial applications were not properly restricted, logged, and monitored. Emergency and temporary access was not properly authorized, and contractor development personnel were granted conflicting access to implement database changes;
        - Complex password configurations were not implemented and\or enforced;
        - User account lists were not periodically reviewed for appropriateness, improper authorizations and excessive user access privileges were allowed at some DHS components, and users were not disabled or removed promptly upon personnel termination; and
        - The process for authorizing and managing virtual private network (VPN) access to external state emergency management agencies, and component contractors, did not comply with DHS and component requirements.
    - Ineffective safeguards over logical and physical access to sensitive facilities and resources.
        - During after-hours physical security walkthroughs, we identified the following unsecured items: Personally Identifiable Information (PII); credit cards; financial system passwords; laptops; sensitive documentation, and server names and IP addresses; and
        - While performing social engineering testing, we identified instances where DHS employees provided their system user names and passwords to an auditor posing as a help desk employee.
    - Lack of generation, review, and analysis of system audit logs and adherence to DHS requirements.
2. *Configuration management:*
    - Lack of documented policies and procedures.

  - Financial systems change control documentation was not updated to represent the current operating environment, including sensitive user functions, roles and privileges;
  - Limited guidance exists to assist in the development of test plans and the completion of functional testing; and
  - Configuration, vulnerability, and patch management plans have not been established and implemented, or did not comply with DHS policy.

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

3. *Security management:*

- Systems certification and accreditation were not completed and maintained, or documented.
  - Several component financial and associated feeder systems as well as general support systems, were not properly certified and accredited, in compliance with DHS policy;
  - Compliance with the Federal Desktop Core Configuration (FDCC) security configurations is in progress, but has not been completed; and
  - System security plans and annual evaluations were not completed and maintained.
- IT Security personnel lack mandatory role-based training or compliance is not documented and monitored.
- Background investigations of federal employees and contractors employed to operate, manage and provide security over IT systems were not being properly conducted.

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.

Related to Financial System Functionality:

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. Financial system functionality limitations also contribute to other control deficiencies reported in our *Independent Auditors' Report* Exhibits I, II, and III, and compliance findings presented in Exhibit IV dated November 11, 2011. We noted persistent and pervasive financial system functionality conditions at all of the significant DHS components in the following general areas:

- Lack of integration between the core financial systems and key feeder systems, such as property management systems, leading to errors and inefficiencies in the processing and reporting of financial data.
- 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 generally accepted accounting principles (GAAP).
- Technical configuration limitations, such as outdated systems that are no longer fully supported by the software vendors, impairing 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 terminated 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.
- Inability to routinely query 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.
- Limitations 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).
- Financial systems functionality limitations are preventing one component from establishing automated processes and application controls that would improve accuracy, reliability, and facilitate efficient processing of certain financial data such as:
    - 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 sufficient data to support Fund Balance with Treasury related transactions, including suspense activity;
    - Maintaining adequate posting logic transaction codes to ensure that transactions are recorded in accordance with GAAP; and
    - Tracking detailed transactions associated with intra-governmental business and eliminating the need for default codes that cannot be easily researched.

Cause/Effect: Many financial system and IT control weaknesses have resulted from DHS' long-standing inability to upgrade its financial system capabilities. The Transformation and Systems Consolidation (TASC) initiative, postponed during FY 2011, is the latest DHS financial systems modernization effort to be postponed, delayed, or canceled. DHS' broad and systemic financial system and IT control limitations will not be fully addressed until DHS and/or the components implement a stable financial system platform. Once a new strategy and plan are developed, it will likely take DHS several years to implement process and system improvements.

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. Many 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), make necessary improvements to the Department's financial management systems and supporting IT security controls.

Appendix A

Description of Key Financial Systems within the Scope of the FY 2011 DHS Financial Statement Audit

Below is a description of significant financial management systems included in the scope of the engagement to perform the financial statement audit.

United States Coast Guard (USCG)

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's Finance Center (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 and the 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 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 (PPC) in Kansas (KS).

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 Operation System Center (OSC) in West Virginia (WV). SAM provides core information about the USCG shore facility assets and facility engineering. The application tracks activities and assists in the management of the Civil Engineering (CE) Program and the Facility Engineering (FE) 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 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 (NC) 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.

Customs and Border Protection (CBP)

SAP Enterprise Central Component (SAP ECC 6.0)

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 6.0 system is located in 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 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 is located in VA.

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 the ACE replace 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, with no set final full deployment date due to funding setbacks. The ACE 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. 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 LAN in a Hybrid physical network topology and are accessible from four sites: Georgia, Washington D.C., 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 (FMS), 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)

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 (COTS) software package developed and maintained by Digital Systems Group Incorporated (DSG). IFMIS-Merger interfaces with Payment and Reporting System (PARS), ProTrac, Smartlink (Department of Health and Human Services), Treasury Information

Executive Repository (TIER) (Department of the Treasury), Secure Payment System (SPS) (Department of the Treasury), Grants Management System (Department of Justice), National Emergency Management Information System (NEMIS), US Coast Guard Credit Card System, Credit Card Transaction Management System (CCTMS), Fire Grants, eGrants, Enterprise Data Warehouse (EDW), and Payroll (Department of Agriculture National Finance Center). IFMIS-Merger is located in VA.

Payment and Reporting System (PARS)

The PARS is a standalone web-based application. The 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 chronological 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 interfaces with IFMIS-Merger and is located in VA.

National Emergency Management Information System (NEMIS)

NEMIS is a FEMA-wide General Support System (GSS) integrating hardware, software, telecommunications infrastructure, and Web-based and client-server services and applications. NEMIS consists of many integrated subsystems distributed over hundreds of separate servers accessed by thousands of client workstations.

NEMIS is an integrated system to provide FEMA, the states, and other Federal agencies with functionality and automation to perform disaster related operations. The subsystems and applications incorporated within NEMIS support all phases of emergency management and provide financial related data to IFMIS via automated interfaces. NEMIS interfaces with IFMIS, US Coast Guard Credit Card System, and the Small Business Administration. The production environment for NEMIS is geographically distributed nationwide but is principally administered and managed in VA.

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 in Maryland. The Traverse client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members.

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.

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 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 (NFC) payroll interface. The FFMS mainframe component and two network servers are hosted at the DHS DC2 facility located in VA. FFMS currently interfaces with the following systems:

- Direct Connect for transmission of DHS payments to Treasury
- Fed Travel
- The Biweekly Examination Analysis Reporting (BEAR) and Controlling Accounting Data Inquiry (CADI), for the purpose of processing NFC user account and payroll information.
- The Debt Collection System (DCOS)
- Bond Management Information System (BMIS) Web

ICE Network

The ICE Network, also known as the Active Directory/Exchange (ADEX) E-mail System, is a major application for ICE and other DHS components, such as the USCIS. The ADEX servers and infrastructure for the headquarters and National Capital Area are located in Washington, DC. 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).

Chief Financial Office VISION (CFO Vision)

CFO Vision is a subsystem of DHSTIER used for the consolidation of the financial data and the preparation of the DHS financial statements. CFO Vision is also administered by RMTO and OFM and is hosted on the DHS OneNet at the Stennis Data Center in 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 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 United States Coast Guard.

Sunflower

Sunflower is a customized third party COTS product used for TSA and Federal Air Marshals 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 United States 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 United States Coast Guard.

United States Citizenship and Immigration Services (USCIS)

CLAIMS 3 Local Area Network (LAN)

CLAIMS3 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, and Administrative Appeals Office. CLAIMS 3 LAN interfaces with the following systems:

- Citizenship and Immigration Services Centralized Oracle Repository (CISCOR)
- CLAIMS 3 Mainframe
- Integrated Card Production System (ICPS)
- CLAIMS 4
- E-filing
- Benefits Biometric Support System (BBSS)
- Refugee, Asylum, and Parole System (RAPS)
- National File Tracking System (NFTS)
- Integrated Card Production System (ICPS)
- Customer Relationship Interface System (CRIS)
- USCIS Enterprise Service Bus (ESB)

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 (RNACS)
- CLAIMS 3 LAN and Mainframe
- Refugee, Asylum, and Parole System (RAPS)
- Enterprise Performance Analysis System (ePAS)
- National File Tracking System (NFTS)
- Asylum Pre-Screening System (APSS)
- USCIS Enterprise Service Bus (ESB)
- Biometrics Benefits Support System (BBSS)
- Enterprise Citizenship and Immigration Service Centralized Operational Repository (eCISOR)
- Customer Relationship Interface System (CRIS)
- FD 258 Enterprise Edition and Mainframe
- Site Profile System (SPS)

Appendix B
FY 2011 Notices of IT Findings and Recommendations at DHS

Notice of Findings and Recommendations (NFR) – Definition of Severity Ratings:

Each NFR listed in appendix B is assigned a severity rating from 1 to 3 indicating the influence on the Department of Homeland Security (DHS) Consolidated Independent Auditors Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist the DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

▪ United States Coast Guard

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
CG-IT-11-01	Security Awareness Issues Associated with Physical Protection of Sensitive Information	Access Controls	2		X
CG-IT-11-02	Direct Access and Direct Access II User and System Administrator Account Management and Approval	Access Controls	1	X	
CG-IT-11-03	Coast Guard Treasury Information Executive Repository (CG TIER) resource owners' identification of authorized users	Access Controls	1		X
CG-IT-11-04	Weaknesses Related to Information Assurance (IA) Professionals' Required Certifications	Security Management	1		X
CG-IT-11-05	Configuration Management Controls over the Scripting Process	Configuration Management	3		X
CG-IT-11-06	Civilian Background Investigations	Security Management	2		X
CG-IT-11-07	Contractor Background Investigations	Security Management	2		X
CG-IT-11-08	Security Awareness Issues Associated with the Social Engineering Testing	Access Controls	2		X
CG-IT-11-09	Operations Systems Center (OSC) Data Center Visitor Access Logs	Access Controls	1	X	
CG-IT-11-10	Direct Access and Direct Access II Audit Logging and General IT Control Validation	Access Controls	2		X
CG-IT-11-11	Aviation Maintenance Management Information System (AMMIS) Software Change Requests Process	Configuration Management	1		X
CG-IT-11-12	Shore Asset Management (SAM) and Naval and Electronics Supply Support System (NESSS) Audit Log Review	Segregation of Duties	1		X
CG-IT-11-13	Direct Access System User Account Recertification	Access Controls	2		X
CG-IT-11-14	NESSS Access Authorizations	Access Controls	2		X
CG-IT-11-15	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Security Management	2		X
CG-IT-11-16	Naval & Electronics Supply Support System Users Who Have Admin Capabilities	Access Controls	2		X
CG-IT-11-17	Aviation Logistics Management Information System (ALMIS)	Access Controls	2		X

	User Recertification				
CG-IT-11-18	Non-Compliance with Federal Financial Management Improvement Act (FFMIA) – Information Technology	Security Management	3		X
CG-IT-11-19	Weaknesses Associated with the Coast Guard Security Incident Database and Ticket System	Security Management	1	X	
CG-IT-11-20	Access and Configuration Management Controls – Vulnerability Assessment	Configuration Management	2	X	
CG-IT-11-21	Naval and Electronics Supply Support System User Account Recertification	Access Controls	2	X	

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

▪ Customs and Border Protection (CBP)

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
CBP-IT-11-01	Security Awareness Issued Identified During Enhanced Security Testing	Access Controls	2		X
CBP-IT-11-02	Physical Security Issues Identified during Enhanced Security Testing	Access Controls	2		X
CBP-IT-11-03	Inadequate Role-based Security Training Program	Entity Level Controls	2		X
CBP-IT-11-04	Segregation of Duties Control Weaknesses within the CBP System	Access Controls	2		X
CBP-IT-11-05	CBP System User Profile Change Logs are not Reviewed	Access Controls	2		X
CBP-IT-11-07	Lack of Monitoring of Developer Emergency/Temporary Access to a CBP System Production	Access Controls	2		X
CBP-IT-11-08	CBP System Novell Server Audit Logs Review Weaknesses	Access Controls	2	X	
CBP-IT-11-09	CBP System Contingency Plan has not been Updated	Computer Operations	1	X	
CBP-IT-11-10	Lack of Update to CBP System Security Plan	Entity Level Controls	2	X	
CBP-IT-11-11	Incomplete Background Investigations and Reinvestigations for CBP Employees and Contractors	Entity Level Controls	2		X
CBP-IT-11-12	Contractor Separation Procedures are not Updated and Contractor Separation Forms are not Maintained	Entity Level Controls	2		X
CBP-IT-11-13	Inadequate Documentation of CBP System Access Change Requests	Access Controls	2		X
CBP-IT-11-14	CBP Systems User Profile Change Logs are not Reviewed	Access Controls	2	X	
CBP-IT-11-15	Incomplete Access Request Forms and Approvals for New CBP System Accounts	Access Controls	2		X
CBP-IT-11-16	Lack of Annual Recertification of CBP System Users	Access Controls	2	X	
CBP-IT-11-17	Incomplete Access Request Approval Forms for new Remote Access User Accounts	Access Controls	2	X	

CBP-IT-11-18	Incomplete Documentation of Interconnection Security Agreements (ISA) for ACS Participating Government Agencies (PGA) Connections	Access Controls	2		X
CBP-IT-11-19	Contractor Non-Disclosure Agreements are Incomplete	Entity Level Controls	2		X
CBP-IT-11-20	Weaknesses over the Employee Separation Process	Entity Level Controls	2		X
CBP-IT-11-21	CBP System Audit Logs Not Appropriately Reviewed	Access Controls	2	X	
CBP-IT-11-22	Lack of Access Requests and Approvals for CBP System Accounts	Access Controls	2		X
CBP-IT-11-23	Lack of Update to CBP System Security Test & Evaluation (ST&E)	Entity Level Controls	2	X	
CBP-IT-11-24	CBP System Configuration Management Policies and Procedures Not Formally Documented	Program Changes	2	X	
CBP-IT-11-25	Weaknesses in Allowed Network Authenticators	Access Controls	2	X	
CBP-IT-11-26	CBP System Audit Logs Not Appropriately Reviewed	Access Controls	2		X
CBP-IT-11-27	Security Weaknesses Identified during the Technical Vulnerability Assessment	Access Controls	2		X
CBP-IT-11-28	Installation of Virus Protections on CBP Workstations	Access Controls	2		X
CBP-IT-11-30	Separated Personnel on CBP System User Listing	Access Controls	2	X	
CBP-IT-11-31	Lack of Functionality in a CBP System	Security Management	2		X
CBP-IT-11-32	Separated Personnel on CBP System User Listing	Access Controls	2	X	
CBP-IT-11-33	Lack of Update to CBP System ST&E	Entity Level Controls	2	X	
CBP-IT-11-34	Lack of Update to CBP System ST&E	Entity Level Controls	2	X	
CBP-IT-11-35	Access to Media Recertification is Incomplete	Access Controls	1		X
CBP-IT-11-36	Lack of Annual Recertification of CBP System Users	Access Controls	2	X	
CBP-IT-11-37	CBP System Privileged User Access Weaknesses	Access Controls	2	X	
CBP-IT-11-38	CBP System Segregation of Duties over the Production Environment	Configuration Management	2	X	

Note: NFR numbers CBP-IT-11-06 and CBP-IT-11-29 were not used during FY2011

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

- **Federal Emergency Management Agency**

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
FEMA-IT-11-01	Alternate Processing Site for the National Emergency Management Information System (NEMIS) Has Not Been Established	Contingency Planning	3		X
FEMA-IT-11-02	Weaknesses Exist in the Certification & Accreditation (C&A) Package for the FEMA Switched Network (FSN)-2, which Includes the FEMA Local Area Network (LAN)	Security Management	3		X
FEMA-IT-11-03	Weaknesses Exist over the Authorization to Operate (ATO) and C&A Documentation for NEMIS	Security Management	3		X
FEMA-IT-11-04	NEMIS Contingency Plan Does Not Comprehensively Address the Requirements of DHS Policy and Has Not Been Adequately Tested	Contingency Planning	3		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	Security Management	2		X
FEMA-IT-11-06	Documentation Supporting Integrated Financial Management Information System (IFMIS)-Merger User Functions Does Not Exist	Configuration Management	2		X
FEMA-IT-11-07	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary are Not Configured to Enforce Password Requirements	Access Controls	2		X
FEMA-IT-11-08	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary Do Not Adequately Enforce Account Lockout Requirements	Access Controls	3		X
FEMA-IT-11-09	Operating System Audit Logging on Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate	Access Controls	3		X
FEMA-IT-11-10	Weaknesses Existed over Contingency Planning, Testing and Development of the Continuity of Operations Plan for the Transaction Record Reporting and Processing Application (TRRP) and Traverse	Contingency Planning	1		X
FEMA-IT-11-11	Recertification of NEMIS Access Control System Position	Access Controls	1		X

	Assignments is Incomplete				
FEMA-IT-11-12	Audit Logging on Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate	Access Controls	3		X
FEMA-IT-11-13	Weaknesses Exist over Vulnerability Management for Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary	Configuration Management	2		X
FEMA-IT-11-14	National Flood Insurance Program (NFIP) Physical Access Policies and Procedures were Not Appropriately Documented and Implemented	Access Controls	2	X	
FEMA-IT-11-15	NFIP LAN and Traverse Account Security Configuration Is Not in Compliance with DHS Policy	Access Controls	1	X	
FEMA-IT-11-16	TRRP Logical Access was Not Appropriately Authorized	Access Controls	2	X	
FEMA-IT-11-17	Weaknesses Exist over Configuration and Operating Effectiveness of Traverse Audit Logs	Access Controls	2	X	
FEMA-IT-11-18	Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment are Inadequate	Configuration Management	3		X
FEMA-IT-11-19	Weaknesses Exist over Configuration Management Processes for Financial Applications within the Previous NEMIS Accreditation Boundary	Configuration Management	3		X
FEMA-IT-11-20	Weaknesses Exist over IFMIS-Merger Configuration Management Processes	Configuration Management	3		X
FEMA-IT-11-21	Weaknesses Exist over Recertification of Access to the IFMIS-Merger Application	Access Controls	3		X
FEMA-IT-11-22	Weaknesses Exist over TRRP Mainframe Audit Logs	Access Controls	2		X
FEMA-IT-11-23	Emergency and Temporary Access to IFMIS-Merger is Not Properly Authorized	Access Controls	2		X
FEMA-IT-11-24	Weaknesses Exist over IFMIS-Merger Application and Database Audit Logging	Access Controls	3		X
FEMA-IT-11-25	IFMIS-Merger User Access was Not Managed in Accordance with Account Management Procedures	Access Controls	1		X
FEMA-IT-11-26	Payment and Reporting System (PARS) Database Security	Access Controls	2		X

	Controls Are Not Appropriately Established				
FEMA-IT-11-27	NFIP LAN Audit Logging is Not Performed in Accordance with DHS and FEMA Requirements	Access Controls	1		X
FEMA-IT-11-28	Individual User Virtual Private Network (VPN) Access Accounts are Not Appropriately Authorized or Recertified	Access Controls	3		X
FEMA-IT-11-29	External Connections to the FEMA VPN Are Not Appropriately Authorized or Documented	Access Controls	3		X
FEMA-IT-11-30	IFMIS-Merger System Software Administrator Activity Is Not Appropriately Restricted or Monitored	Access Controls	3		X
FEMA-IT-11-31	Weaknesses Exist over C&A Documentation for IFMIS-Merger	Security Management	3		X
FEMA-IT-11-32	Risk Assessment Activities over NFIP IT Systems were Not Adequately Performed	Security Management	2		X
FEMA-IT-11-33	Weaknesses Exist over Management and Technical Controls Associated with FEMA LAN Accounts	Access Controls	1		X
FEMA-IT-11-34	Employee Termination Process for Removing System Access Should Be More Proactive	Access Controls	3		X
FEMA-IT-11-35	Traverse Configuration Management Plan Weaknesses	Configuration Management	2		X
FEMA-IT-11-36	TRRP Configuration Management Plan Weaknesses	Configuration Management	2		X
FEMA-IT-11-37	Documentation Supporting TRRP Test Libraries Does Not Reflect Current Environment	Configuration Management	1	X	
FEMA-IT-11-38	Federal Insurance and Mitigation Administration (FIMA) Configuration Management Program has Not Been Developed	Configuration Management	2	X	
FEMA-IT-11-39	Weaknesses Exist over Background Investigations for Federal Employees and Contractors	Security Management	2		X
FEMA-IT-11-40	Weaknesses in the Management of Plans of Action & Milestones (POA&Ms) for Audit Findings over FEMA Financial Systems	Security Management	3		X
FEMA-IT-11-41	Physical Security and Security Awareness Issues Associated with Enhanced Security Testing at FEMA	Access Controls	2		X
FEMA-IT-11-42	Traverse Accounts Were Not Appropriately Recertified	Access Controls	2	X	
FEMA-IT-11-43	Lack of Adequate Configuration Management over Network	Configuration Management	2		X

	Devices Supporting Financial Systems				
FEMA-IT-11-44	Password, Patch, and Configuration Management Weaknesses Were Identified during the Vulnerability Assessment on IFMIS, NEMIS, and Key Support Servers	Configuration Management	3	X	
FEMA-IT-11-45	Vulnerability Assessment Program for the NFIP LAN Supporting Traverse was Inadequate	Configuration Management	1		X
FEMA-IT-11-46	Weaknesses Existed over the Configuration Patch Management Process for the NFIP LAN Supporting Traverse	Configuration Management	1		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	Contingency Planning	3		X
FEMA-IT-11-48	Key Controls over Production Servers Supporting Applications Within the Former NEMIS Accreditation Boundary Have Not Been Implemented	Configuration Management	3		X

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

▪ Federal Law Enforcement Training Center

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
FLETC-IT-11-01	Ineffective Logical Access Controls over Student Information System	Access Controls	2		X
FLETC-IT-11-02	Ineffective Segregation of Duties Controls for the Momentum System	Segregation of Duties	2	X	

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

▪ Immigration and Customs Enforcement

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
ICE-IT-11-01	ADEX Resource Servers and Workstations have Inadequate Patch Management	Access Controls	3	X	
ICE-IT-11-02	Terminated/Transferred Personnel are not Removed from ADEX in a Timely Manner	Access Controls	2		X
ICE-IT-11-03	Access Recertification Review is not Completed for FFMS.	Access Controls	2	X	
ICE-IT-11-04	Weak FFMS Segregation of Duties	Access Controls	2		X
ICE-IT-11-05	Security Awareness Issues were Identified during Social Engineering	Security Management	3		X
ICE-IT-11-06	FFMS Network and Servers were Installed with Default Configuration Settings and Protocols	Access Controls	3		X
ICE-IT-11-07	FFMS Mainframe Production Databases were Installed and Configured without Baseline Security Configurations	Access Controls	3		X
ICE-IT-11-08	FFMS Servers have Inadequate Patch Management	Access Controls	3		X
ICE-IT-11-09	Default Installation and Configuration of Cisco Routers on ICE Network	Access Controls	3		X
ICE-IT-11-10	Security Awareness Issues Identified During After-Hours Walkthrough	Security Management	3		X
ICE-IT-11-11	Lack of Procedures for Transferred/Terminated Personnel Exit Processing	Security Management	2		X

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

- **Office of Financial Management**
- **Office of Chief Information Officer**

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
CONS-IT-11-01	Network Logical Access Parameters are not Configured in Accordance with DHS Policy	Access Controls	1		X
CONS-IT-11-02	Security Awareness Issues Identified During After-Hours Walkthrough	Security Management	2	X	
OCIO-IT-11-01	DHS has not Fully Implemented the Federal Desktop Core Configuration (FDCC) Security Configurations Requirements	Security Management	1		X
OCIO-IT-11-02	DHS Physical Controls could be Strengthened	Access Controls	2	X	

Department of Homeland Security
FY2011 Information Technology - Notice of Findings

▪ Transportation Security Administration

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
TSA-IT-11-01	Markview – Password Settings	Access Controls	2	X	
TSA-IT-11-02	Markview – Administrator Account	Access Controls	2	X	
TSA-IT-11-03	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing	Access Controls	1		X
TSA-IT-11-04	TSA Computer Access Agreement Process	Access Controls	1		X
TSA-IT-11-05	Sunflower and Markview User Account Recertifications	Access Controls	2		X
TSA-IT-11-06	Configuration Management Controls Over the Coast Guard Scripting Process	Configuration Management	2		X

Department of Homeland Security
FY2011 Information Technology
Notice of Findings

- **United States Citizenship and Immigration Services**

Appendix B

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

2011 NFR #	NFR Title	FISCAM Control Area	Severity Rating	New Issue	Repeat Issue
CIS-IT-11-01	Equipment and Media Policies and Procedures are not Current	Access Controls	2		X
CIS-IT-11-02	Weak Password Configuration Controls for CLAIMS 4	Access Controls	2		X
CIS-IT-11-03	Policies and Procedures for CLAIMS 3 LAN and CLAIMS 4 Audit Logs	Access Controls	2		X
CIS-IT-11-04	Policies and Procedures for Separated CLAIMS 3 LAN Accounts	Access Controls	2		X
CIS-IT-11-05	Periodic User Access Reviews are not Performed for CLAIMS 3 LAN Users	Access Controls			X
CIS-IT-11-06	Procedures for Transferred/Terminated Personnel Exit Processing are not Finalized	Security Management	3		X
CIS-IT-11-07	Incomplete or Inadequate Access Request Forms for CLAIMS 3 LAN and CLAIMS 4 System Users	Access Controls	2		X
CIS-IT-11-08	ICE Resource Server and Inadequate Patch Management weaknesses impact USCIS Operations	Access Controls	3		X
CIS-IT-11-09	Weak Password configuration controls for CLAIMS 3 LAN	Access Controls	2	X	
CIS-IT-11-10	Weak Logical Access Controls exist over CLAIMS 4	Access Controls	2		X
CIS-IT-11-11	Ineffective Safeguards over Physical Access to Sensitive Facilities and Resources	Access Controls	2	X	
CIS-IT-11-12	VPN Access Request Forms are not Properly Maintained	Access Controls	2	X	
CIS-IT-11-13	Lack of Segregation of Duties for CLAIMS 3 LAN	Security Management	2		X
CIS-IT-11-14	ADEX Access Request Forms are not Properly Maintained	Access Controls	1		X
CIS-IT-11-15	Lack of Computer Security Awareness Training Compliance	Security Management	2		X
CIS-IT-11-16	Lack of Role-Based Training for Key Security Personnel	Security Management	2	X	
CIS-IT-11-17	FFMS Vulnerability Weaknesses Affect USCIS Operations	Access Controls	3		X

APPENDIX C

Status of Prior Year Notices of Findings and Recommendations and Comparison to

Current Year Notices of Findings and Recommendations at DHS

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

Current Year Notices of Findings and Recommendations

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
CBP-IT-10-01	Separated Personnel on Automated Commercial Environment (ACE) User Listings	X	
CBP-IT-10-02	Segregation of Duties Control Weaknesses within ACE		X
CBP-IT-10-03	ACE Audit Log Review Weaknesses		X
CBP-IT-10-05	Recertification Review of ACE User Accounts	X	
CBP-IT-10-06	Security Awareness Issues Identified During Enhanced Security Testing		X
CBP-IT-10-07	ACE User Access Form Documentation is Incomplete		X
CBP-IT-10-08	Physical Security Issues Identified during Enhanced Security Testing		X
CBP-IT-10-09	Contractor Separation procedures are not Updated and Contractor Separation forms are not Maintained		X
CBP-IT-10-10	Employee Separations Weaknesses		X
CBP-IT-10-11	Contractor Non-Disclosure Agreement Weaknesses		X
CBP-IT-10-12	Installation of Virus Protections on CBP Workstations		X
CBP-IT-10-13	Inadequate Role-based Security Training Program	X	
CBP-IT-10-14	Raised Floor Access Authorization Process Weakness		X
CBP-IT-10-15	Automated Commercial System (ACS) User Access Profile Change Log Review Procedures Have Not Been Implemented		X
CBP-IT-10-16	Security Weaknesses Identified during Technical Vulnerability Assessment		X
CBP-IT-10-17	ACS Interconnection Security Agreements are Incomplete		X
CBP-IT-10-18	ACS User Access Authorization Evidence Weakness		X
CBP-IT-10-19	Lack of Recertification Authorization Evidence for Personnel with Access to Backup Media		X
CBP-IT-10-20	ACS User Access Profile Change Log Review Procedures Have Not Been Implemented	X	
CBP-IT-10-21	Unauthorized Access Attempt Setting for the Mainframe Have Not Been Configured		X
CBP-IT-10-22	Background Investigations and Reinvestigations for CBP Employees and Contractors are not Completed		X
CBP-IT-10-23	Lack of Monitoring of Developer Emergency/Temporary Access to ACS Production		X
CBP-IT-10-24	Lack of Access Requests and Approval for National Data Center (NDC) Local Area Network (LAN) Accounts		X
CG-IT-10-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Process for Coast Guard Systems		X
CG-IT-10-02	Contractor Background Investigations		X
CG-IT-10-03	Civilian Background Investigations		X
CG-IT-10-04	Lack of Implemented Guidance Related to Financial Statement Impact Assessment within the Change Control Process	X	
CG-IT-10-05	Configuration Management Controls Over the Scripting Process		X
CG-IT-10-06	Security Awareness Issues Associated with the Social		X

	Engineering Testing		
CG-IT-10-07	JUMPS Authorized Users Tracking Weakness	X	
CG-IT-10-08	Coast Guard – Treasury Information Executive Reporting (TIER) System – Password Settings	X	
CG-IT-10-09	Security Awareness Issues Associated with Physical Protection of Sensitive Information		X
CG-IT-10-10	Weaknesses with Specialized Role-based Training for Individuals with Significant Security Responsibilities		X
CG-IT-10-11	Coast Guard Treasury Information Executive Repository (CG TIER) Resource Owners' Identification of Authorized Users		X
CG-IT-10-12	User Account Recertification - Direct Access Application		X
CG-IT-10-13	Access and Configuration Management Controls – Vulnerability Assessment	X	
CG-IT-10-14	Naval and Electronic Supply Support System (NESSS) Access Authorizations		X
CG-IT-10-15	Aviation Logistics Center (ALC) Data Center and Facility Controls	X	
CG-IT-10-16	Aviation Maintenance Management Information System (AMMIS) Password Configuration	X	
CG-IT-10-17	Security Awareness Issues associated with Social Engineering Testing – Follow-up Testing		X
CG-IT-10-18	AMMIS Audit Log Review	X	
CG-IT-10-19	Aviation Logistics Management Information System (ALMIS) User Recertification		X
CG-IT-10-20	AMMIS Software Change Requests Process		X
CG-IT-10-21	NESSS User Access Recertification		X
CG-IT-10-22	Shore Asset Management (SAM) and NESSS Audit Log Review		X
CG-IT-10-23	Operations Systems Center (OSC) Data Center Access Reviews	X	
CG-IT-10-24	Non-Compliance with Federal Financial Management Improvement Act (FFMIA) – Information Technology		X
CG-IT-10-25	FINCEN Configuration Management Testing Approval Process	X	
CG-IT-10-26	ALC Information Technology Policies and Procedures	X	
CG-IT-10-27	NESSS Password Configuration	X	
CG-IT-10-28	Direct Access Audit Logging		X
CIS-IT-10-01	Inefficient Definition and Documentation of Access roles at the National Benefits Center for CLAIMS 3 LAN		X
CIS-IT-10-02	Periodic User Access Reviews are not Performed for CLAIMS 3 LAN users		X
CIS-IT-10-03	Incomplete or Inadequate Access Request Forms for CLAIMS 3 LAN and CLAIMS 4 System Users		X
CIS-IT-10-04	Procedures for Transferred/Terminated Personnel Exit Processing are not Finalized		X
CIS-IT-10-05	Equipment and Media Policies and Procedures are not Current		X
CIS-IT-10-06	FFMS Vulnerability Weaknesses Impact USCIS Operations		X
CIS-IT-10-07	Weak Password Configuration Controls for CLAIMS 4		X
CIS-IT-10-08	Ineffective Safeguards over Physical Access to Sensitive Facilities and Resources	X	
CIS-IT-10-09	Lack of Policies and Procedures for CLAIMS 3 LAN and CLAIMS 4 Audit Logs		X

CIS-IT-10-10	Weak Logical Access Controls Exist over CLAIMS 4		X
CIS-IT-10-11	Lack of Policies and Procedures for Separated CLAIMS 3 LAN Accounts		X
CIS-IT-10-12	IT Security Awareness Training Compliance is not Monitored		X
CIS-IT-10-13	ADEX Access Request Forms are not Properly Maintained.		X
CIS-IT-10-14	Default Installation and Configuration of Cisco routers on ICE Network Impact USCIS Operations		X
CONS-IT-10-01	Network Logical Access Parameters are not Configured in Accordance with DHS policy		X
FEMA-IT-10-01	Recertification of National Emergency Management Information System (NEMIS) Access Control System Position Assignments is Incomplete		X
FEMA-IT-10-02	Alternate Processing Site for NEMIS Has Not Been Established		X
FEMA-IT-10-03	End-User Workstation Screensaver Configuration is Not Sufficient	X	
FEMA-IT-10-04	Operating System Audit Logging on Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate		X
FEMA-IT-10-05	Payment and Reporting System (PARS) Database Security Controls Are Not Appropriately Established		X
FEMA-IT-10-06	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary are Not Configured to Enforce Password Requirements		X
FEMA-IT-10-07	Integrated Financial Management Information System (IFMIS)-Merged Oracle Database is Not Configured to Prevent the Reuse of Passwords	X	
FEMA-IT-10-08	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary Do Not Adequately Enforce Account Lockout Requirements		X
FEMA-IT-10-09	Audit Logging on Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate		X
FEMA-IT-10-10	Inadequate FEMA Contractor Tracking Program	X	
FEMA-IT-10-11	Weaknesses Exist over IFMIS-Merger Application and Database Audit Logging		X
FEMA-IT-10-12	Grants & Training (G&T) IFMIS Access Authorizations Were Not Consistently Documented	X	
FEMA-IT-10-13	G&T IFMIS Oracle Database Auditing Was Not Sufficient	X	
FEMA-IT-10-14	Weaknesses Exist over Recertification of Access to the IFMIS-Merger Application		X
FEMA-IT-10-15	Recertification of G&T IFMIS Application and Database Access Recertification Was Not Performed	X	
FEMA-IT-10-16	G&T IFMIS Was Not Certified and Accredited	X	
FEMA-IT-10-17	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-10-18	Weaknesses Exist over the Authorization to Operate (ATO) and		X

	Certification & Accreditation (C&A) Documentation for NEMIS		
FEMA-IT-10-19	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems		X
FEMA-IT-10-20	NEMIS Contingency Plan Does Not Comprehensively Address the Requirements of DHS Policy and Has Not Been Adequately Tested		X
FEMA-IT-10-21	Employee Termination Process for Removing System Access Should Be More Proactive		X
FEMA-IT-10-22	Weaknesses Exist over Management and Technical Controls Associated with FEMA Local Area Network (LAN) Accounts		X
FEMA-IT-10-23	Weaknesses Existed over the Configuration Patch Management Process for the National Flood Insurance Program (NFIP) LAN Supporting Traverse		X
FEMA-IT-10-24	Risk Assessment Activities over NFIP IT Systems were Not Adequately Performed		X
FEMA-IT-10-25	Individual User Virtual Private Network (VPN) Access Accounts are Not Appropriately Authorized or Recertified		X
FEMA-IT-10-26	IFMIS-Merger User Access was Not Managed in Accordance with Account Management Procedures		X
FEMA-IT-10-27	G&T IFMIS Oracle Database Security Controls Were Not Configured Properly	X	
FEMA-IT-10-28	Weaknesses Exist in the C&A Package for the FEMA Switched Network (FSN)-2, which Includes the FEMA LAN		X
FEMA-IT-10-29	The PARS Has Not Been Certified and Accredited	X	
FEMA-IT-10-30	Emergency and Temporary Access to IFMIS-Merger is Not Properly Authorized		X
FEMA-IT-10-31	Weaknesses Exist in FEMA's Incident Response Capability	X	
FEMA-IT-10-32	G&T IFMIS and IFMIS-Merger Patch Management Weaknesses	X	
FEMA-IT-10-33	Weaknesses Exist over Vulnerability Management for Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary		X
FEMA-IT-10-34	Weaknesses Exist over Vulnerability Management for G&T IFMIS and IFMIS-Merger	X	
FEMA-IT-10-35	Weaknesses Exist over NEMIS Patch Management Guidance	X	
FEMA-IT-10-36	Weaknesses Exist over the Configuration and Testing of Backups for Servers Supporting Financial Applications Within the Previous NEMIS Accreditation Boundary		X
FEMA-IT-10-37	Security Awareness Issues Associated with Social Engineering Testing at FEMA	X	
FEMA-IT-10-38	Physical Security and Security Awareness Issues Associated with Enhanced Security Testing at FEMA		X
FEMA-IT-10-39	Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment are Inadequate		X
FEMA-IT-10-40	System Programmers Had the Ability to Migrate Code into the G&T IFMIS Production Environment	X	
FEMA-IT-10-41	Password, Patch, and Configuration Management Weaknesses Were Identified during the Vulnerability Assessment on IFMIS, NEMIS, and Key Support Servers	X	
FEMA-IT-10-42	Weaknesses Exist over C&A Documentation for IFMIS-Merger		X
FEMA-IT-10-43	Weaknesses Exist over the ATO and C&A Documentation for		X

	NEMIS		
FEMA-IT-10-44	IFMIS-Merger System Software Administrator Activity Is Not Appropriately Restricted or Monitored		X
FEMA-IT-10-45	Weaknesses Exist over Background Investigations for Federal Employees and Contractors		X
FEMA-IT-10-46	Key Controls over Production Servers Supporting Applications Within the Former NEMIS Accreditation Boundary Have Not Been Implemented		X
FEMA-IT-10-47	FEMA Management Needs to Improve Planning, Management, and Communication Related to Financial Systems Development and Acquisition Projects	X	
FEMA-IT-10-48	Weaknesses in the Management of Plans of Action & Milestones (POA&Ms) for Audit Findings over FEMA Financial Systems		X
FEMA-IT-10-49	Documentation Supporting IFMIS-Merger User Functions Does Not Exist		X
FEMA-IT-10-50	External Connections to the FEMA VPN Are Not Appropriately Authorized or Documented		X
FEMA-IT-10-51	NEMIS Access Restrictions to Program Directories within the Test and Development Laboratory (TDL) Needs Improvement	X	
FEMA-IT-10-52	Vulnerability Assessment Program for the NFIP LAN Supporting Traverse was Inadequate		X
FEMA-IT-10-53	Transaction Record Reporting and Processing (TRRP) Mainframe Access Accounts Are Not Periodically Reviewed	X	
FEMA-IT-10-54	Inadequate Implementation of DHS Systems Engineering Life Cycle (SELC) Requirements for the IFMIS-Merger Project	X	
FEMA-IT-10-55	NFIP LAN Audit Logging is Not Performed in Accordance with DHS and FEMA Requirements		X
FEMA-IT-10-56	Weaknesses Exist over TRRP Mainframe Audit Logs		X
FEMA-IT-10-57	Lack of Formal Processes for Managing Remote Access to the LAN Supporting the TRRP Mainframe	X	
FEMA-IT-10-58	Traverse Configuration Management Plan Weaknesses		X
FEMA-IT-10-59	TRRP Configuration Management Plan Weaknesses		X
FEMA-IT-10-60	Weaknesses Exist over the Implementation of Traverse System Changes	X	
FEMA-IT-10-61	Weaknesses Existed over Contingency Planning, Testing and Development of the Continuity of Operations Plan (COOP) for TRRP and Traverse		X
FEMA-IT-10-62	Weaknesses Exist over Configuration Management Processes for Financial Applications within the previous NEMIS Accreditation Boundary		X
FEMA-IT-10-63	Weaknesses Exist over IFMIS-Merger Configuration Management Processes		X
FLETC-IT-10-01	A Configuration Management Plan has not been fully implemented	X	
FLETC-IT-10-02	Ineffective Logical Access Controls over the Glynco Administrative Network (GAN)	X	
FLETC-IT-10-03	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing	X	
FLETC-IT-10-04	GAN audit logs are not reviewed	X	

FLETC-IT-10-05	Weak Access Controls around Momentum	X	
FLETC-IT-10-06	Ineffective Logical Access Controls over Student Information System (SIS)		X
ICE-IT-10-01	Procedures for Transferred/Terminated Personnel Exit Processing are not Followed		X
ICE-IT-10-02	Ineffective Password Settings in FFMS	X	
ICE-IT-10-03	Formal Policy for FFMS Access Recertification is not Documented and Approved	X	
ICE-IT-10-04	Weak FFMS Segregation of Duties		X
ICE-IT-10-05	Audit Log Policies and Procedures are not Documented for FFMS	X	
ICE-IT-10-06	Terminated/Transferred Personnel are not Removed from ADEX in a Timely Manner		X
ICE-IT-10-07	Weak Environmental Controls at the OCS Datacenter	X	
ICE-IT-10-08	Weak Environmental Controls at the PCN Computer Room	X	
ICE-IT-10-09	Security Awareness Issues Identified during Social Engineering		X
ICE-IT-10-10	Security Awareness Issues Identified during After-Hours Walkthrough		X
ICE-IT-10-11	Training for IT security Personnel is not Mandatory.	X	
ICE-IT-10-12	Physical Safeguard Weaknesses exist at DHS DC2 Datacenter	X	
ICE-IT-10-13	FFMS Network and Servers were Installed with Default Configuration Settings and Protocols		X
ICE-IT-10-14	FFMS Mainframe Production Databases were Installed and Configured without Baseline Security Configurations.		X
ICE-IT-10-15	FFMS Servers have Inadequate Patch Management		X
ICE-IT-10-16	Default Installation and Configuration of Cisco Routers on ICE Network		X
OCIO-IT-10-01	DHS has not Fully Implemented the Federal Desktop Core Configuration (FDCC) Security Configurations Requirements		X
OCIO-IT-10-02	DHS Policies and Procedures Need Clarity	X	
TSA-IT-10-01	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		X
TSA-IT-10-02	Core Accounting System (CAS), Financial Procurement Desktop (FPD), and Sunflower Access Recertifications		X
TSA-IT-10-03	TSA Computer Access Agreement Process		X
TSA-IT-10-04	Configuration Management Controls Over the Coast Guard Scripting Process		X

Department of Homeland Security
Information Technology Management Letter
September 30, 2011

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary, Management
Chief Information Officer
Chief Financial Officer
Chief Information Security Officer
Assistant Secretary, Policy
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to Department of Homeland Security programs and operations:

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

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