Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2011 DHS Financial Statement Audit

OIG-12-70

April 2012

Office of Inspector General

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

April 5, 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 Federal Emergency Management Agency (FEMA) component of the FY 2011 DHS consolidated 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 procedures at the FEMA component in support of the DHS FY 2011 consolidated 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 conclusions 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

February 22, 2012

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
U.S. Federal Emergency Management Agency

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, based on the criteria established in Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Internal Control, Appendix A*. 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.

Our *Independent Auditors' Report* issued on November 11, 2011, describes a limitation on the scope of our audit that prevented us from performing all procedures necessary to express an unqualified opinion on DHS' FY 2011 financial statements and internal control over financial reporting. In addition, the FY 2011 DHS *Secretary's Assurance Statement* states that the Department was unable to provide assurance that internal control over financial reporting was operating effectively at September 30, 2011.

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

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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

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

OBJECTIVE, SCOPE, AND APPROACH

We have audited the U.S. Department of Homeland Security's (DHS or Department) balance sheet as of September 30, 2011, and the related statement of custodial activity for the year then ended. We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2011 and the statement of custodial activity for the year then ended. During our fiscal year (FY) 2011 financial statement audit, we performed an evaluation of general information technology (IT) controls (GITC) at the Federal Emergency Management Agency (FEMA). The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A.

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 GITC 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 provide 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, as well as testing over certain key financial application controls in the FEMA environment. The technical security testing was performed from within a select FEMA facility and focused on production devices that directly support FEMA's financial processing and key general support systems. Limited social engineering and after-hours physical security testing was also included in the scope of technical security testing.

In addition to testing FEMA's general control environment, we performed application control tests on a limited number of FEMA's financial systems and applications, specifically those supporting the National Flood Insurance Program (NFIP). The application control testing was performed to

assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2011, FEMA took corrective action to address certain prior year IT control weaknesses. For example, FEMA made improvements over implementing certain logical controls over FEMA and NFIP information systems, as well as development and implementation of controls around patch management and vulnerability management. Additionally, we noted improvement in the areas of certain IT entity-level controls, including those related to incident response and handling, contractor management, and IT investment life cycle management. However, during FY 2011, we continued to identify IT general control weaknesses that could potentially impact FEMA's financial data. The most significant weaknesses from a financial statement audit perspective related to controls over security management, access control, configuration management, and contingency planning for the Integrated Financial Management Information System (IFMIS)-Merger, financial applications within the previous National Emergency Management Information System accreditation boundary (hereinafter referred to as "NEMIS"), Payment and Reporting System (PARS), Traverse, Transaction Record Reporting and Processing (TRRP), and associated General Support System (GSS) environments, as well as weaknesses over physical security and security awareness.

Collectively, the IT control weaknesses limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over FEMA financial reporting and its operation, and we consider them to collectively contribute to a material weakness at the DHS level under standards established by the American Institute of Certified Public Accountants (AICPA). In addition, based upon the results of our test work, we noted that FEMA did not fully comply with the requirements of the *Federal Financial Management Improvement Act of 1996* (FFMIA).

Of the 48 findings identified during our FY 2011 testing, 40 were repeat findings, either partially or in whole from the prior year, and 8 were new IT findings. These findings represent weaknesses in each of the five FISCAM key control areas.

The majority of findings resulted from the lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program,* requirements and National Institute of Standards and Technology (NIST) guidance. Specifically, the findings stem from: 1) the lack of formal designation of financial system security responsibilities, 2) inadequately designed and operating access control policies and procedures relating to the management of access to financial applications, databases, and support systems, and supervisor recertification of user access privileges, 3) insufficient logging of system events and monitoring of audit logs, 4) inadequately designed and operating configuration management policies and procedures, 5) patch, configuration, and vulnerability management control deficiencies within the system, 6) financial systems that were not properly certified and accredited and authorized to operate, and 7) the lack of adequately documented or tested contingency plans. These weaknesses may increase the risk that the

confidentiality, integrity, and availability of system controls and FEMA financial data could be exploited; thereby compromising the integrity of FEMA financial data used by management and reported in the DHS financial statements.

While the recommendations made by us should be considered by FEMA, it is the ultimate responsibility of FEMA management to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2011 DHS financial statement audit, we identified the following IT and financial system control deficiencies at FEMA that collectively contribute to an IT material weakness at the Department level. Our findings focused on financial systems controls as testing over IT system functionality could not be conducted.

Configuration Management

- Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting IFMIS-Merger, NEMIS, and general support systems;
- Formal procedures for conducting internal scans of servers supporting NEMIS did not define requirements or procedures to ensure that system owners are aware of, and appropriately execute, responsibilities associated with vulnerability management for the system components under their area of responsibility. Additionally, vulnerabilities identified on NEMIS system components were not consistently tracked or monitored via the Plan of Actions & Milestones (POA&M) process;
- Formalized configuration management plans for NEMIS and IFMIS-Merger were not documented to ensure that changes were adequately and centrally controlled, documented, or managed throughout the lifecycle of the FEMA configuration management process;
- No formalized change management procedures existed for the use of shared accounts for deploying changes to the NEMIS production environment or to ensure that the movement of production code for NEMIS is appropriately controlled or monitored. Additionally, evidence could not be provided that management had appropriately restricted and controlled access to the NEMIS production application, web, and database servers for the deployment of changes;
- Configuration management policies and procedures did not include comprehensive requirements for the frequency, documentation, and performance of monitoring audits for configuration baselines for all relevant network devices such as firewalls, routers, and switches that support financial systems to ensure that configuration items (CIs) within the scope of financial systems are documented and monitored in accordance with FEMA policy. Additionally, configuration changes which were implemented over these devices were not consistently or adequately documented or authorized;
- A formalized process for modifying IFMIS-Merger system security functions to ensure that appropriate privileges are created, documented, approved, and monitored did not exist;

- Formal procedures were not implemented to require monitoring of changes deployed to IFMIS-Merger program libraries to review and validate implemented changes. Furthermore, informal reviews of developer activities that were conducted did not provide enough information to ensure that the approved changes were implemented;
- For a majority of the fiscal year, formal procedures for conducting internal scans of the NFIP Local Area Network (LAN) supporting Traverse did not incorporate all components of the system environment to ensure that scans were properly conducted and monitored by FEMA or NFIP contractor management. Additionally, a formal process did not exist for the remediation of vulnerabilities identified during internal scans to ensure that the vulnerabilities were tracked and monitored via the POA&M process;
- The configuration management plans for Traverse and TRRP did not comprehensively provide guidance to address all configuration management control elements required by FEMA and DHS policy for standard and emergency changes;
- TRRP changes were not approved prior to development and implementation into production;
- Formalized processes were not properly or comprehensively documented and implemented to ensure that FEMA management within the Federal Insurance and Mitigation Administration (FIMA), Risk Insurance Division (RID), were adequately involved in configuration management activities over Traverse and TRRP;
- Documentation supporting the logical components of the TRRP environment was not current or complete; and
- For a majority of the fiscal year, documented change management procedures did not include requirements for approving, testing, and ensuring timely installation of operating system patches for all components of the NFIP LAN supporting Traverse.

Security Management

- Policies and procedures requiring the completion and tracking of specialized training for FEMA employees and contractors identified as possessing significant information security responsibilities had not been fully implemented as required by DHS policy;
- Certification and accreditation (C&A) activities for IFMIS-Merger and the NFIP IT environment were not completed in accordance with DHS and NIST requirements;
- The FEMA Switch Network (FSN)-2 C&A package was not completed in compliance with DHS and NIST requirements and had not been updated to reflect the current operating environment. Additionally, the Authorization to Operate (ATO) expired in January 2010 and was not renewed. As a result, the FSN-2 GSS was operating without a valid ATO;

- Although the FSN-2 C&A package references various subsystems supporting and hosting IFMIS and NEMIS, FEMA management was unable to identify and confirm the FSN-2 subsystems (including regional LANs) that host all the production servers for NEMIS and IFMIS applications;
- Documentation associated with the C&A package for NEMIS, including the system security plan (SSP) and ATO, expired and was not renewed;
- IT security management responsibilities were not consistently or adequately assigned and performed over the FEMA POA&M process for FY 2010 IT audit findings, in accordance with DHS guidance; and
- Suitability investigations for FEMA Federal employees and contractors accessing DHS IT systems were not appropriately conducted, and results were not properly documented or tracked.

After-Hours Physical Security Testing:

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to media and equipment that housed financial data and information residing on a FEMA employee's / contractor's desk which could be used by others to gain unauthorized access to systems housing financial information. The specific results are listed below:

Exceptions Noted	FEMA Locations Tested			Total Exceptions by Type
	Washington Design Center	Patriots Plaza	FEMA Finance Center	
Passwords	3	6	13	**22**
For Official Use Only (FOUO)	2	2	0	**4**
Keys	0	0	0	**0**
Personally Identifiable Information (PII)	6	2	2	**10**
Unlocked Laptops	3	1	1	**5**
Server Names/ IP Addresses	1	1	0	**2**
Credit Cards	0	0	0	**0**
Classified Documents	0	0	0	**0**
Unlocked Workstations	1	0	0	**1**
Total by Location	**16**	**12**	**16**	**44**

Social Engineering Testing:

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing/enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering or gaining computer system access. During the social engineering testing, while several personnel provided us with user IDs, no passwords were divulged or compromised. The specific results of our testing are documented in the following table:

Testing Date	Total Called	Total Answered	Number of Personnel Who Provided Their User ID and Password	Number of Personnel Who Provided Their User ID Only	Number of Personnel Who Provided Their Password Only
06/02/2011	45	17	0	10	0
07/13/2011	35	8	0	6	0

Access Controls

- Procedures for managing and periodically reviewing physical access to the facility hosting the NFIP LAN and Traverse were not formally documented or implemented and did not require documentation of periodic reviews for a majority of the fiscal year. Additionally, physical access privileges were not consistently or properly authorized;
- IFMIS-Merger, NEMIS, Traverse, and PARS application and/or database accounts, network accounts, and remote user accounts were not periodically reviewed for appropriateness and/or were not fully and accurately recertified in accordance with FEMA and DHS policy, resulting in inappropriate authorizations and excessive user access privileges;
- IFMIS-Merger and NEMIS application accounts, network accounts, and remote user accounts were not disabled or removed promptly upon personnel termination;
- Initial and modified access granted to TRRP application and FEMA network and remote users was not properly documented and authorized;
- Documented procedures for auditing NEMIS, IFMIS-Merger, and PARS databases were not comprehensive and did not meet DHS requirements. Additionally, for these financial systems, the NFIP LAN, Traverse, and TRRP, logging of operating system, application, and/or database events required to be recorded were not enabled for some or all of the events, audit logs were not appropriately reviewed and/or were reviewed by those with conflicting roles, and evidence of audit log reviews was not retained;
- The Standard Operating Procedure (SOP) for monitoring sensitive access to NEMIS operating system software was not implemented and did not include all operating

system servers that were within the scope of the previous NEMIS accreditation boundary. Additionally, no application or tool was in place to support the audit logging function on the NEMIS servers;

- Strong password requirements were not enforced on the NEMIS databases, the NFIP LAN, or Traverse;
- FEMA's process for authorizing and managing remote virtual private network (VPN) access to external state emergency management agencies and FEMA contractors did not comply with DHS and FEMA requirements. Specifically, existing documentation did not define the requirements for administering the site survey process with external organizations seeking VPN access or identify FEMA roles and responsibilities for managing VPN access granted to external individuals using non-DHS equipment to access the FEMA network;
- Two-factor authentication was not used for VPN access, as required by DHS policy;
- System administrator root access to IFMIS-Merger was not properly restricted, logged, and monitored; and
- Emergency and temporary access to the IFMIS-Merger databases was not properly authorized.

Segregation of Duties – we identified segregation of duties weaknesses associated with other FISCAM areas. Specifically, weaknesses in those areas pertain to access controls over audit log reviews and configuration management controls for migrating code into production. See those respective sections for additional information.

Contingency Planning

- Documented procedures that outline processes for performing backups of NEMIS production databases and for rotating and physically securing backup tapes off-site had not been formally defined;
- NEMIS backup tapes were not regularly tested in accordance with FEMA and DHS policy;
- An alternate processing site for NEMIS was not established and implemented. Additionally, an exception to DHS policy for the lack of an established alternate processing site, as required for systems such as NEMIS that are categorized as "high impact" for availability, had not been requested by FEMA (this weakness is enhanced due to the control deficiencies noted above associated with performance and testing of NEMIS data backups);
- The most recent NEMIS contingency plan had expired and had not been revised or approved by FEMA management. Additionally, full scale testing of the NEMIS contingency plan was not conducted;

- For a majority of the fiscal year, the existing NFIP LAN and Traverse contingency plan was not updated or tested in compliance with DHS and NIST requirements; and
- The FIMA RID Continuity of Operations Plan (COOP), including Traverse and TRRP, was not formally documented or approved until June 2011.

Recommendations:

We recommend that the FEMA Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the DHS OCFO and the DHS OCIO, make the following improvements to FEMA's financial management systems and associated information technology security program.

For Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the Notice of Finding and Recommendation (NFR) that was issued for deficiencies identified during our vulnerability assessment;
- Develop, finalize, and ensure that formal procedures are understood and implemented by system owners for all NEMIS system components under their area of responsibility for: conducting periodic internal vulnerability scans of all components of the system and assessing, reporting, tracking, and monitoring correction of vulnerabilities identified during internal scans;
- Develop and implement formal configuration management plans for NEMIS and IFMIS-Merger to control emergency and non-emergency changes to financial systems application software, and ensure consistent adherence with requirements for approving, testing, documenting, properly controlling and tracking changes, and retaining related documentation;
- Document and implement a formalized process and procedures for deploying NEMIS changes to ensure that access to the NEMIS production application, web, and database servers, including the use of shared accounts for movement of production code for the NEMIS production environment, is appropriately controlled and monitored;
- Revise and fully implement configuration management policies and procedures over documenting and maintaining current baseline configurations for network devices supporting financial applications, including IFMIS-Merger, to ensure DHS and FEMA requirements are adequately addressed, configuration baselines are comprehensively documented, and configuration changes to network devices are consistently documented and authorized by FEMA. Additionally, policies and procedures should include guidance over requirements such as roles and responsibilities, documentation of baselines, periodic review and auditing, and approval of baseline changes for network devices;

- Develop and implement formal procedures for conducting periodic reviews of changes deployed to IFMIS-Merger program libraries to verify that only authorized changes are implemented into production and for retaining evidence of reviews conducted on file;
- Update the current versions of Traverse and TRRP configuration management plans and procedures to comprehensively address DHS and FEMA requirements; procedures should fully incorporate FIMA RID management in required configuration management activities and establish a process for conducting, validating, documenting, and approving tests of configuration changes prior to implementation as well as conducting post-deployment verification activities. Additionally, ensure the consistent implementation of configuration management procedures for all changes to Traverse and TRRP;
- Update TRRP system documentation to fully reflect all current system components, including logical datasets associated with the production and test environments; and
- Fully implement comprehensive patch management policies and procedures to ensure that required operating system patches for all components of the NFIP LAN supporting Traverse are authorized, tested, and implemented.

For Security Management

- Fully implement policies and procedures requiring initial and periodic specialized training for individuals with significant information security responsibilities to ensure that training requirements for all individuals possessing specific roles and positions associated with significant information security responsibilities are tracked;
- Document or update all required C&A artifacts for NEMIS, IFMIS-Merger, Traverse, TRRP, the NFIP LAN, and FSN-2 in accordance with DHS policy and NIST guidance. Additionally, ensure that C&A artifacts, including the risk assessment or the results of the required risk assessment activities, the Security Testing and Evaluation (ST&E), and the Security Assessment Report (SAR) are conducted and documented over all components of the systems in accordance with established DHS baseline controls according to the security categorization of the system;
- Establish and document a formalized process to provide IT security management oversight to ensure that adequate periodic review and assessment of security controls are performed and corrective actions are appropriately assigned and implemented over identified security weaknesses through the POA&M process;
- Further refine processes to ensure that background investigations for all types of Federal employees and contractors are consistently performed and centrally tracked in accordance with DHS policy;
- Review the effectiveness of existing security awareness programs designed to protect "need-to-know" information, including IT system access credentials, electronic and

physical data, PII, and FOUO agency information, and ensure that individuals are adequately instructed and reminded of their roles in the protection of sensitive system information from unauthorized individuals through formal, periodic communications and/or security awareness training.

For Access Controls

- Fully establish and/or implement user account management recertification processes and require completion of periodic reviews of all user accounts for appropriate access and documentation of current user profiles for IFMIS-Merger, NEMIS, Traverse, and PARS; the FEMA network and remote user accounts; and physical access to the facility hosting the computer room supporting the NFIP LAN and the Traverse application. The processes should include revocation of accounts or access privileges that cannot be verified during recertification processes;
- Update, as necessary, and consistently implement procedures and processes to ensure that all system accounts, including remote access accounts, of terminated employees and contractors are immediately removed/disabled upon their departure;
- Review and revise existing procedures to require documented authorization of new and modified user accounts by supervisors, program managers, and contracting officers' technical representatives in accordance with DHS requirements;
- Revise and implement detailed procedures requiring the consistent and timely review of IFMIS-Merger, NEMIS, PARS, NFIP LAN, Traverse, and TRRP database, application, and operating system logs and the maintenance of documentation supporting such reviews in accordance with DHS requirements. These procedures should also incorporate segregation of duties principles;
- Configure audit logs for financial databases and applications to ensure that auditable events, as required by DHS policy, are recorded and appropriately reviewed by personnel without conflicting duties, and sufficient evidence is retained;
- Revise, implement, and ensure adherence to the SOP for monitoring sensitive access to NEMIS operating system software to ensure that the scope of the procedures includes all defined NEMIS servers, and deploy the appropriate tool(s) to support audit logging functions on the NEMIS servers, in accordance with FEMA and DHS policy;
- Configure NEMIS databases and NFIP LAN and Traverse accounts to enforce strong password and authenticator control requirements, and ensure that individuals with system/database administration and security responsibilities are aware of and properly trained in DHS, FEMA, and Federal requirements;
- Revise and implement policies and procedures for documenting, reviewing, and approving the security controls in place over non-DHS equipment connecting to the FEMA network via VPN access, and ensure that roles, responsibilities, and security requirements for authorizing and managing VPN access for external organizations

connecting to the FEMA network are defined and implemented in accordance with DHS and FEMA policy;

- Implement two-factor authentication for all remote access to the FEMA network;
- Develop and implement policies and procedures that document the process of adding, deleting, and modifying IFMIS-Merger security functions to ensure that the proper controls are in place for modifying user account privileges. Additionally, ensure that the use of function modification privileges is monitored;
- Develop and implement procedures for monitoring IFMIS system administrator and highly-privileged account activities and restricting access to the root account, and ensure that reviews of system logs and records are properly conducted; and
- Consistently implement a formal process for granting IFMIS-Merger emergency and temporary database access that includes segregation of duties considerations and appropriate approval from FEMA management, as required by DHS policy.

For Contingency Planning

- Complete on-going efforts to establish and implement an alternate processing site for NEMIS;
- Ensure that a formal process is established, documented, and implemented to fully backup all necessary components of the NEMIS databases, secure backup media off-site, and periodically test NEMIS backup media at a frequency that is in accordance with FEMA and DHS policy; and
- Update the NEMIS contingency plan in accordance with DHS requirements for high impact availability systems, inclusive of accurate system architecture information; conduct documented annual tests of the plan; and as necessary, update the plan with lessons learned from testing.

APPLICATION CONTROLS

We concluded that application controls over NEMIS, IFMIS-Merger, and PARS could not be relied upon for purposes of our FY 2011 audit procedures because of the nature of the general IT control deficiencies identified and discussed above. As a result, we did not test application controls for these financial systems. However, we conducted certain application control testing over key financial systems supporting NFIP. Based on the testwork conducted, we did not identify any findings in the area of application controls related to NFIP during the FY 2011 DHS financial statement audit.

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

Appendix A

Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2011 DHS Financial Statement Audit

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

Below is a description of significant Federal Emergency Management Agency (FEMA) financial management systems and supporting information technology (IT) infrastructure included in the scope of the Department of Homeland Security (DHS) fiscal year (FY) 2011 financial statement audit.

Locations of Testing FEMA Headquarters in Washington, D.C.; the Mount Weather Emergency Operations Center in Virginia; IT operations in Virginia; the National Flood Insurance Program (NFIP) in Virginia; and the NFIP contractor location in Maryland.

Systems Subject to Audit:

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 (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), U.S. 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 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 cron 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 Virginia.

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-Merger via automated interfaces. NEMIS interfaces with IFMIS-Merger, U.S. Coast Guard Credit Card System, and Small Business Administration. The production environment for NEMIS is geographically distributed nationwide but is principally administered and managed in Virginia.

Traverse

Traverse is the general ledger application currently used by the National Flood Insurance Program (NFIP) Bureau and Statistical Agent to generate the NFIP financial statements. Traverse is a client-server application that runs on the NFIP Local Area Network (LAN) Windows server environment in Maryland. The Traverse client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members. Traverse has no known 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.

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

Appendix B

FY 2011 Notices of IT Findings and Recommendations at the FEMA

Appendix B

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

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 ratings are provided only to assist the Federal Emergency Management Agency (FEMA) in prioritizing the development of its corrective action plans for remediation of the deficiency.

Appendix B

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

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 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

Appendix B

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

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
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 (TRRP) Application and Traverse	Contingency Planning	1		X
FEMA-IT-11-11	Recertification of NEMIS Access Control System Position Assignments is Incomplete	Access Controls	1		X
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

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

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
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 Controls Are Not Appropriately Established	Access Controls	2		X
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

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

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
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	

Appendix B

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

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
FEMA-IT-11-43	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems	Configuration Management	2		X
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
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2010

Appendix C

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

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2010

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-10-01	Recertification of National Emergency Management Information System (NEMIS) Access Control System Position Assignments is Incomplete		FEMA-IT-11-11
FEMA-IT-10-02	Alternate Processing Site for NEMIS Has Not Been Established		FEMA-IT-11-01
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		FEMA-IT-11-09
FEMA-IT-10-05	Payment and Reporting System (PARS) Database Security Controls Are Not Appropriately Established		FEMA-IT-11-26
FEMA-IT-10-06	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary are Not Configured to Enforce Password Requirements		FEMA-IT-11-07
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		FEMA-IT-11-08
FEMA-IT-10-09	Audit Logging on Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate		FEMA-IT-11-12
FEMA-IT-10-10	Inadequate FEMA Contractor Tracking Program	X	
FEMA-IT-10-11	Weaknesses Exist over IFMIS-Merger Application and Database Audit Logging		FEMA-IT-11-24
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		FEMA-IT-11-21
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		FEMA-IT-11-05
FEMA-IT-10-18	Weaknesses Exist over the Authorization to Operate (ATO) and Certification & Accreditation (C&A) Documentation for NEMIS		FEMA-IT-11-03
FEMA-IT-10-19	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems		FEMA-IT-11-43
FEMA-IT-10-20	NEMIS Contingency Plan Does Not Comprehensively Address the Requirements of DHS Policy and Has Not Been Adequately Tested		FEMA-IT-11-04
FEMA-IT-10-21	Employee Termination Process for Removing System Access Should Be More Proactive		FEMA-IT-11-34

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2010

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-10-22	Weaknesses Exist over Management and Technical Controls Associated with FEMA Local Area Network (LAN) Accounts		FEMA-IT-11-33
FEMA-IT-10-23	Weaknesses Existed over the Configuration Patch Management Process for the National Flood Insurance Program (NFIP) LAN Supporting Traverse		FEMA-IT-11-46
FEMA-IT-10-24	Risk Assessment Activities over NFIP IT Systems were Not Adequately Performed		FEMA-IT-11-32
FEMA-IT-10-25	Individual User Virtual Private Network (VPN) Access Accounts are Not Appropriately Authorized or Recertified		FEMA-IT-11-28
FEMA-IT-10-26	IFMIS-Merger User Access was Not Managed in Accordance with Account Management Procedures		FEMA-IT-11-25
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		FEMA-IT-11-02
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		FEMA-IT-11-23
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		FEMA-IT-11-13
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		FEMA-IT-11-47
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		FEMA-IT-11-41
FEMA-IT-10-39	Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment are Inadequate		FEMA-IT-11-18
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		FEMA-IT-11-31
FEMA-IT-10-43	Weaknesses Exist over the ATO and C&A Documentation for NEMIS		FEMA-IT-11-03
FEMA-IT-10-44	IFMIS-Merger System Software Administrator Activity Is Not Appropriately Restricted or Monitored		FEMA-IT-11-30

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2010

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-10-45	Weaknesses Exist over Background Investigations for Federal Employees and Contractors		FEMA-IT-11-39
FEMA-IT-10-46	Key Controls over Production Servers Supporting Applications Within the Former NEMIS Accreditation Boundary Have Not Been Implemented		FEMA-IT-11-48
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		FEMA-IT-11-40
FEMA-IT-10-49	Documentation Supporting IFMIS-Merger User Functions Does Not Exist		FEMA-IT-11-06
FEMA-IT-10-50	External Connections to the FEMA VPN Are Not Appropriately Authorized or Documented		FEMA-IT-11-29
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		FEMA-IT-11-45
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		FEMA-IT-11-27
FEMA-IT-10-56	Weaknesses Exist over TRRP Mainframe Audit Logs		FEMA-IT-11-22
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		FEMA-IT-11-35
FEMA-IT-10-59	TRRP Configuration Management Plan Weaknesses		FEMA-IT-11-36
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		FEMA-IT-11-10
FEMA-IT-10-62	Weaknesses Exist over Configuration Management Processes for Financial Applications within the previous NEMIS Accreditation Boundary		FEMA-IT-11-19
FEMA-IT-10-63	Weaknesses Exist over IFMIS-Merger Configuration Management Processes		FEMA-IT-11-20

Report Distribution

Department of Homeland Security

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