Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2013 Department of Homeland Security Financial Statement Audit

OIG-14-76

April 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 24, 2014

MEMORANDUM FOR: Adrian Gardner
Chief Information Officer
Federal Emergency Management Agency

Edward Johnson
Chief Financial Officer
Federal Emergency Management Agency

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

SUBJECT: *Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2013 Department of Homeland Security Financial Statement Audit*

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

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

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

Attachment

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

March 11, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Department of Homeland Security Federal Emergency Management Agency

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated December 11, 2013, included internal control deficiencies identified during our audit that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to the Federal Emergency Management Agency (FEMA).

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and communicated through Notices of Findings and Recommendations (NFRs), are intended to improve internal control or result in other operating efficiencies and are summarized as described below.

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

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

During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of DHS' organization gained during our work to make comments and suggestions that we hope will be useful to you.

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

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

Very truly yours,

KPMG LLP

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2013

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	**2**
Summary of Findings	**4**
General IT Control Findings and Recommendations	**6**
Findings	**6**
Security Management	**6**
Access Controls	**6**
Configuration Management	**7**
Segregation of Duties	**7**
Contingency Planning	**7**
Recommendations	**8**
Security Management	**8**
Access Controls	**8**
Configuration Management	**9**
Segregation of Duties	**9**
Contingency Planning	**9**
IT Application Controls	**10**

APPENDICES

Appendix	Subject	Page
A	Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit	**11**
B	FY 2013 IT Notices of Findings and Recommendations at FEMA	**15**

OBJECTIVE, SCOPE, AND APPROACH

Objective

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

Scope

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

Approach

General Information Technology Controls

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

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

- *Security Management* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.

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

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

- *Configuration Management* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.

- We performed technical information security testing for key FEMA network and system devices. The technical security testing was performed from within select DHS facilities and focused on production devices that directly support DHS' and FEMA's financial processing and key general support systems.

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

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

IT Application Controls

We performed testing over selected key IT application controls on financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions. FISCAM defines application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS

During FY 2013, FEMA took corrective action to address certain prior year IT control deficiencies. For example, FEMA made improvements over designing and implementing certain configuration management and security authorization controls over FEMA information systems, as well as strengthening and improving controls around vulnerability management and logical access controls. However, during FY 2013, we continued to identify GITC deficiencies related to controls over security management (including deficiencies over physical security and security awareness), access control, configuration management, segregation of duties, and contingency planning for FEMA core financial and feeder systems and associated General Support System environments.

Collectively, the IT control deficiencies 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 deficiencies negatively impacted FEMA's internal controls over financial reporting and its operations. We consider these deficiencies, in aggregate, to contribute to the IT material weakness at the Department level under standards established by the American Institute of Certified Public Accountants. In addition, based upon the results of our test work, we noted that FEMA contributes to the Department's non-compliance with the relevant federal financial management systems requirements of the *Federal Financial Management Improvement Act of 1996.*

Of the 28 IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, 26 were repeat findings, either partially or in whole from the prior year, and 2 were new findings. The 28 IT NFRs issued represent deficiencies in all five FISCAM GITC categories.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, requirements and National Institute of Standards and Technology (NIST) guidance. Specifically, the findings stem from:

1. Improper or incomplete security authorization activities and supporting artifacts and documentation;
2. Insufficient logging of system events and monitoring of audit logs;
3. Inadequately designed and ineffective access control policies and procedures relating to the management of logical access to financial applications, databases, and support systems;
4. Patch, configuration, and vulnerability management control deficiencies within systems;
5. Inadequately designed and ineffective configuration management policies and procedures; and
6. The lack of alternate processing capabilities.

These deficiencies 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 FEMA's and 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 deficiencies identified.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following FEMA GITC and IT entity-level control deficiencies that, in the aggregate, contribute to the IT material weakness at the Department level. Those FEMA GITC deficiencies that we determined to be "more significant" in posing a risk to the integrity of FEMA financial data are identified in Appendix B.

Security Management

- Individuals with significant information security oversight and management responsibilities subject to role-based training were not fully identified by management, and compliance with specialized training requirements was not consistently tracked.

- Security authorization activities and supporting documentation and artifacts for the Integrated Financial Management Information System (IFMIS), Non-Disaster Grants (NDGrants), and Emergency Support (ES) – including Authorization to Operate (ATO) memoranda, risk assessments, privacy threshold analyses, security plans, IT contingency plans (CPs) and associated plan test results, security control assessments, Security Assessment Reports, and corresponding Plans of Action and Milestones – were not completed in accordance with DHS and NIST requirements.

After-Hours Physical Security Testing

On July 2 and July 11, 2013, 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 printed or electronic media, equipment, or credentials residing within a FEMA employee's or contractor's work area or shared workspaces which could be used by others to gain unauthorized access to systems housing financial or other sensitive information. The testing was performed at various FEMA locations in the Washington, DC, metropolitan area that process, maintain, and/or have access to financial data.

We observed 78 instances where passwords, sensitive IT information (such as server names or IP addresses), unsecured or unlocked laptops and external media, and printed materials marked "For Official Use Only" or containing sensitive Personally Identifiable Information were accessible by individuals without a "need to know".

Access Controls

- Audit logs for components of the IFMIS environment (including the application, operating system, and IFMIS and Payment and Reporting System (PARS) databases) were not consistently reviewed by management in accordance with DHS policy (including the issue that audit records were not generated to demonstrate evidence of review on dates without relevant security activities), and IFMIS audit logging policies and procedures were outdated.

- Controls to generate, and perform and document independent reviews of, required audit records of events on NDGrants, Emergency Management Mission Integrated Environment (EMMIE), and ES were not implemented.

- Strong password requirements were not enforced on the NDGrants, EMMIE, and ES databases, and documentation supporting exceptions to DHS password requirements was incomplete.

- Procedures for managing access to the NDGrants, EMMIE, and ES applications did not adequately identify elevated privileges within the systems or controls to review and authorize access to such privileges.

- Account management activities on FEMA financial applications (IFMIS, NDGrants, EMMIE, and ES) and supporting databases, including authorization of new and modified access, were not consistently or timely documented or implemented in accordance with DHS and FEMA policy.

Configuration Management

- Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting IFMIS, NDGrants, EMMIE, the National Flood Insurance Program (NFIP) Local Area Network (LAN), and financially significant segments of the FEMA Enterprise Network (FEN) and end-user computing environment.

- Controls to validate the completeness and integrity of changes to the IFMIS, NDGrants, EMMIE, and ES production environments were not implemented.

- Configuration management policies, procedures, and processes for documenting and implementing configuration changes to FEN network devices were not finalized and approved for a majority of the year, or fully implemented.

- Documentation supporting the approval and testing of configuration changes to the IFMIS environment was not consistently maintained.

Segregation of Duties

- FEMA personnel with financial reporting, management, and oversight roles were granted IFMIS application access that was excessive and/or not consistent with the principles of least privilege and segregation of duties, and existing system documentation did not adequately define the implementation of certain access groups and associated privileges granted to these personnel.

Contingency Planning

- Alternate processing sites for NDGrants, EMMIE, and ES were not established; consequently, testing of those systems' CPs, including restoration to an established alternate processing site, was not performed.

Recommendations

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

Security Management

- Develop and implement monitoring controls over background investigation processes to ensure that investigations for all types of Federal employees and contractors are consistently performed and centrally tracked in accordance with DHS policy.

- Enhance existing policies and procedures related to initial and periodic specialized training for individuals with significant information security responsibilities and implement additional monitoring controls to ensure that all individuals possessing specific roles and positions associated with significant information security responsibilities are identified and compliance with training requirements is tracked.

- Document or update all required security authorization artifacts for IFMIS, NDGrants, and ES in accordance with DHS policy and NIST guidance, and revise and implement appropriate monitoring controls to ensure continued compliance with applicable criteria related to security authorization activities and supporting documentation.

- Continue existing efforts to formally document and implement controls and relevant policies and procedures, including conducting periodic checks of FEMA workspaces and enforcing employee sanctions as appropriate, to ensure that sensitive DHS and FEMA data are secured properly in accordance with DHS requirements.

Access Controls

- Develop and implement monitoring controls over the audit log review process on the IFMIS application, operating system, and the IFMIS and PARS database logs to ensure that audit logs are reviewed by management on a periodic basis and are documented, and audit log review evidence is maintained in accordance with FEMA and DHS requirements.

- Configure audit logs for the NDGrants, EMMIE, and ES databases and applications to ensure that auditable events are recorded at an appropriate level of detail to attribute activity to individual users, retained, and appropriately reviewed by independent security management personnel.

- Implement technical controls to ensure that passwords for NDGrants, EMMIE, and ES databases accounts are configured in accordance with FEMA and DHS requirements. If necessary and justified by operational and business requirements, ensure that requests for exceptions from DHS password requirements clearly document all affected user and service accounts subject to deviations from standard controls.

- Review and revise existing system documentation and procedures to identify elevated privileges within the NDGrants, EMMIE, and ES applications and controls to review and authorize access to such privileges.

- Develop and implement monitoring controls over the account management process to ensure that all users are granted access to FEMA system(s) in accordance with FEMA and DHS requirements.

Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during our vulnerability assessments.

- Implement formal technical and management controls to systematically track and review modifications to the IFMIS, NDGrants, EMMIE, and ES production environments to ensure the completeness and integrity of change reports and logs.

- Fully implement configuration management policies and procedures to ensure that configuration changes to FEN network devices are consistently documented and authorized by FEMA management in accordance with DHS policy and the FEN configuration management plan.

- Develop and implement monitoring controls over the IFMIS configuration management process to ensure that changes deployed to the IFMIS production environment are properly approved and tested, and sufficient evidence is retained.

Segregation of Duties

- Document and implement controls to manage the assignment of groups and corresponding roles and functionality within the IFMIS application by identifying conflicting roles, revising system documentation as appropriate, and analyzing and modifying existing assignments to address violations of segregation of duties and least privilege principles.

Contingency Planning

- Dedicate resources to complete actions associated with the migration of FEMA systems to the DHS Enterprise Data Center; formally establish and implement controls around alternate processing capabilities for NDGrants, EMMIE, and ES; and conduct and document the results of tests of those systems' CPs, including simulated recovery from contingency events at the designated alternate processing site(s).

IT APPLICATION CONTROLS

We concluded that application controls over IFMIS, NDGrants, EMMIE, ES, and PARS could not be relied upon for purposes of our FY 2013 audit procedures because of the nature of the GITC deficiencies identified and discussed above. As a result, we did not test application controls for these financial systems.

However, during the FEMA component of the FY 2013 DHS financial statement audit we did conduct testing over certain application controls on key financial systems supporting NFIP and did not identify any control deficiencies.

Appendix A

Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit

Below is a description of significant FEMA financial management systems and supporting IT infrastructure included in the scope of the FEMA component of the DHS FY 2013 financial statement audit.

Integrated Financial Management Information System (IFMIS)

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

Payment and Reporting System (PARS)

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

Non-Disaster Grant Management System (NDGrants)

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

Emergency Management Mission Integrated Environment (EMMIE)

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

process amendments, and conduct close-out activities. Interfaces exist between the EMMIE system, IFMIS, and ISAAC. EMMIE is located in VA.

Emergency Support (ES)

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

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

ES is located in VA.

Traverse

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

Transaction Recording and Reporting Processing (TRRP)

The TRRP application acts as a central repository of all data submitted by the Write Your Own (WYO) companies and the Direct Servicing Agent (DSA) for the NFIP. TRRP also supports the WYO program,

primarily by ensuring the quality of financial data submitted by the WYO companies and DSA to TRRP. TRRP is a mainframe-based application that runs on the NFIP mainframe logical partition in Connecticut. TRRP has no known system interfaces.

Appendix B
FY 2013 IT Notices of Findings and Recommendations at FEMA

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue	More Significant[1]
FEMA-IT-13-01	Non-Compliance with Alternate Processing Site Requirements for Key Financial Systems	Contingency Planning		X	X
FEMA-IT-13-02	Insufficient Audit Log Controls for Key Financial Systems	Access Controls		X	X
FEMA-IT-13-03	Inconsistent Implementation of DHS Background Investigation Requirements for FEMA Federal Employees and Contractors	Security Management		X	
FEMA-IT-13-04	Incomplete Implementation of Role-Based Training for Individuals with Significant Information Security Responsibilities	Security Management		X	
FEMA-IT-13-05	Non-Compliant Security Authorization Package for NDGrants	Security Management		X	
FEMA-IT-13-06	Non-Compliance with DHS and FEMA Password Requirements for Oracle Databases Supporting Certain Financial Applications	Access Controls		X	
FEMA-IT-13-07	Incomplete Exception Request for Password Controls on Oracle Databases Supporting Certain Financial Applications	Security Management[2]			
FEMA-IT-13-08	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management	X	X	
FEMA-IT-13-09	Weaknesses Identified during the Vulnerability Assessment on IFMIS	Access Controls; Configuration Management		X	X
FEMA-IT-13-10	Weaknesses Identified during the Vulnerability Assessment on the NFIP LAN	Access Controls; Configuration Management		X	X

[1] NFRs designated as "More Significant" represent control deficiencies that we determined to pose an increased risk to the integrity of FEMA financial data.
[2] NFR FEMA-IT-13-07 was reported in conjunction with FEMA-IT-13-06 as part of GITC deficiencies related to access controls in our *Independent Auditors' Report* dated December 11, 2013.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2013

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue	More Significant[1]
FEMA-IT-13-11	Weaknesses Identified during the Vulnerability Assessment on Financially Significant Segments of the FEMA Enterprise Network and End-User Computing Environment	Configuration Management		X	X
FEMA-IT-13-12	Weaknesses Identified during the Vulnerability Assessment on EMMIE	Configuration Management		X	
FEMA-IT-13-13	Weaknesses Identified during the Vulnerability Assessment on NDGrants	Access Controls; Configuration Management		X	X
FEMA-IT-13-14	Non-Compliant Security Authorization Package for ES	Security Management		X	
FEMA-IT-13-15	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for EMMIE, NDGrants, and ES	Configuration Management		X	X
FEMA-IT-13-16	Incomplete Account Management Documentation for the EMMIE Application	Access Controls	X		X
FEMA-IT-13-17	Incomplete Account Management Documentation for NDGrants	Access Controls		X	X
FEMA-IT-13-18	Incomplete Account Management Documentation for ES	Access Controls		X	X
FEMA-IT-13-19	Excessive or Inappropriate Access to IFMIS	Access Controls; Segregation of Duties			X
FEMA-IT-13-20	Lack of EMMIE System Owner Approval for Database Accounts	Access Controls		X	X
FEMA-IT-13-21	Lack of ES System Owner Approval for Database Accounts	Access Controls	X	X	
FEMA-IT-13-22	Lack of NDGrants System Owner Approval for Database Accounts	Access Controls		X	X
FEMA-IT-13-23	Inconsistent Authorization of New and Modified IFMIS Application User Access	Access Controls		X	X
FEMA-IT-13-24	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems	Configuration Management		X	

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue	More Significant[1]
FEMA-IT-13-25	Inconsistent Activities and Incomplete Documentation Supporting Configuration Changes for the IFMIS Application	Configuration Management		X	X
FEMA-IT-13-26	Inconsistent Review of IFMIS Audit Logs	Access Controls		X	X
FEMA-IT-13-27	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the IFMIS Production Environment	Configuration Management		X	X
FEMA-IT-13-28	Non-Compliant Security Authorization Package for IFMIS	Security Management	X		

Appendix A
Report Distribution

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

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

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

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

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

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