

Department of Homeland Security **Office of Inspector General**

Information Technology Management Letter for the
Federal Emergency Management Agency Component
of the FY 2012 Department of Homeland Security
Financial Statement Audit





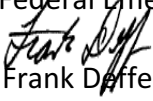
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 4, 2013

MEMORANDUM FOR: Ken Murphy
Acting Chief Information Officer
Federal Emergency Management Agency

Edward Johnson
Chief Financial Officer
Federal Emergency Management Agency

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

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

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

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

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

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



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

April 2, 2013

Inspector General
U.S. Department of Homeland Security

Acting 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, 2012, and the related statements of net cost, changes in net position, and custodial activity, and combined statement of budgetary resources for the year then ended (referred to as the “fiscal year (FY) 2012 financial statements”). We were also engaged to audit the Department’s internal control over financial reporting of the FY 2012 financial statements. The objective of our audit engagement was to express an opinion on the fair presentation of the FY 2012 financial statements and the effectiveness of internal control over financial reporting of the FY 2012 financial statements.

In accordance with *Government Auditing Standards*, our *Independent Auditors’ Report*, dated November 14, 2012, included internal control deficiencies identified during our audit engagement 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 engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to FEMA’s financial systems general IT controls (GITC) which we believe contribute to a DHS Department-wide material weakness in IT controls and financial system functionality. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

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



This report is intended solely for the information and use of DHS management, DHS OIG, U.S. Office of Management and Budget, 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, 2012

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	1
Summary of Findings and Recommendations	2
General IT Control Findings and Recommendations	4
<i>Findings</i>	4
Configuration Management	4
Security Management	5
<i>After – Hours Physical Security Testing</i>	5
Access Controls	6
Segregation of Duties	7
Contingency Planning	7
<i>Recommendations</i>	7
Configuration Management	7
Security Management	8
Access Controls	8
Contingency Planning	9
Application Controls	11

APPENDICES

Appendix	Subject	Page
A	Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2012 DHS Financial Statement Audit Engagement	12
B	FY 2012 Notices of IT Findings and Recommendations at FEMA	16
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at FEMA	21

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit the financial statements of DHS as of and for the year ended September 30, 2012, we performed an evaluation of the general Information Technology (IT) controls (GITCs) at FEMA to assist in planning and performing our audit engagement. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. 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 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 functions to be essential to the effective operation of GITCs and the IT environment:

- *Security Management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access Control (AC)* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and 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 and testing over certain key financial application controls in the FEMA environment. The technical security testing was performed from within select FEMA and contractor facilities and focused on production devices that directly support FEMA's financial processing and key general support systems. Limited after-hours physical security testing was also included in the scope of technical security testing.

In addition to testing FEMA's GITC 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 financial systems' internal controls over the input, processing, and output of financial data and transactions.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2012, FEMA took corrective action to address certain prior year IT control weaknesses. For example, FEMA made improvements over designing and implementing certain physical and logical access controls over FEMA and NFIP information systems, as well as strengthening and improving controls around patch management and vulnerability management. However, during FY 2012, we continued to identify GITC and entity-level control weaknesses that could potentially impact FEMA's financial data.

FEMA Office of the Chief Financial Officer (OCFO) and Office of the Chief Information Officer (OCIO) management informed us that the management conducted a quantitative and qualitative analysis of the composite functions, capabilities, applications, and subsystems previously included within the accreditation boundary of the General Support System (GSS) previously accredited as the National Emergency Management Information System (NEMIS). As a result of that analysis and our planning considerations, Non-Disaster Grants (ND Grants), Emergency Support (ES), and the Emergency Management Mission Integrated Environment (EMMIE) were identified as financially significant information systems subject to controls test work during the FY 2012 audit. Consequently, findings issued in FY 2011 which related to the previous NEMIS accreditation boundary were determined to be no longer applicable to FEMA's control environment and were closed. Test work was performed specific to these three systems to determine the status of corrective actions implemented to address the prior year NEMIS-related conditions.

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, Payment and Reporting System (PARS), ND Grants, ES, EMMIE, Traverse, Transaction Record Reporting and Processing (TRRP), and associated General Support System (GSS) environments including the FEMA Enterprise Network (FEN), 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. 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*.

Of the 61 findings identified during our FY 2012 testing, 16 were repeat findings, either partially or in whole from the prior year, and 45 were new IT findings. While 32 of 48 prior year findings were closed in FY 2012, as noted above, 11 were closed solely because of the decoupling of the previous NEMIS accreditation boundary into its constituent financial systems. Through our test work we noted that weaknesses existed in the 3 financially significant decoupled systems in the control areas related to these prior year findings, and as a result, 29 new findings were issued. Further, 9 prior year NFRs closed were based on improvements noted in the design and implementation of certain controls, which enabled us to test the operating effectiveness of the control. However, this additional test work highlighted

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

inconsistencies in control implementation, resulting in 9 new findings being issued. The 61 findings issued represent weaknesses in each of the five FISCAM key control areas.

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

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.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following FEMA GITC control deficiencies that in the aggregate contribute to the IT material weakness at the Department level.

Configuration Management

- Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting IFMIS-Merger, NDGrants, EMMIE, Traverse, and the NFIP Local Area Network (LAN), and financially significant segments of the FEN and end-user computing environment.
- Formal procedures for conducting internal scans of servers supporting FEMA systems did not define requirements or procedures to ensure that system owners document reviews of scan results. Additionally, internal scans over ES system components were not consistently performed.
- A formalized configuration management plan (CMP) for ES was not documented to ensure that changes were adequately and centrally controlled, documented, or managed throughout the lifecycle of the FEMA configuration management process, and the CMPs for EMMIE and NDGrants did not fully document all control activities necessary to support the review and approval of changes to those systems.
- The use of shared accounts for deploying changes to the NDGrants and EMMIE production environments was not properly authorized, controlled or monitored, and controls to validate the integrity and completeness of changes to those systems were not designed or implemented properly.
- 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 IFMIS-Merger to ensure that configuration items within the scope of the system accreditation boundary 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.
- Formal procedures to require monitoring of changes deployed to IFMIS-Merger program libraries to review and validate implemented changes did not accurately reflect existing technical controls and processes related to configuration management activities within the production environment. Furthermore, reviews of developer activities were not consistently conducted for changes implemented during FY 2012.
- Formal procedures for conducting internal scans of the NFIP LAN supporting Traverse did not include requirements for tracking and monitoring all types of vulnerabilities via the Plan of Actions & Milestones (POA&M) process.
- A testing environment did not exist to validate changes to Traverse software prior to deployment to production.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

- TRRP and IFMIS-Merger changes were not consistently tested or approved prior to development and implementation into production.

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 and identification of applicable personnel subject to specialized training requirements had not been fully implemented as required by DHS policy.
- Security authorization activities and supporting documentation and artifacts for IFMIS-Merger, FEN, EMMIE, NDGrants, and ES – including Authorization to Operate (ATO) memoranda, risk assessments, privacy threshold analyses, security plans, IT contingency plans (CP) and associated plan test results, security control assessments, Security Assessment Reports (SAR) and corresponding POA&Ms – were not completed in accordance with DHS and NIST requirements.
- IT security management responsibilities were not consistently or adequately assigned and performed over the FEMA POA&M process for FY 2011 IT audit findings, in accordance with DHS guidance.
- Background 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:

On May 29 and June 6, 2012, 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 within a FEMA employee’s or contractor’s work area which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various FEMA locations that process and/or maintain financial data. The specific results are listed in the following table:

Exceptions Noted	FEMA Locations Tested			Total Exceptions by Type
	Washington Design Center	Patriots Plaza	FEMA Finance Center	
Passwords	19	18	2	39
For Official Use Only (FOUO)	3	3	0	6
Keys	0	0	0	0
Personally Identifiable Information (PII)	10	0	3	13
Unlocked Laptops	5	1	13	19
Server Names/ IP Addresses	1	0	0	1
Credit Cards	0	0	0	0
Classified Documents	0	0	0	0
Unsecured External Media	0	0	1	1

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

Exceptions Noted	FEMA Locations Tested			Total Exceptions by Type
	Washington Design Center	Patriots Plaza	FEMA Finance Center	
Unlocked Interior Office	1	0	0	1
Total by Location	39	22	19	80

Access Controls

- Traverse application accounts were not periodically recertified at an appropriate level of detail to determine the continued appropriateness of user access and associated privileges and system functionality.
- FEN accounts were not disabled or removed promptly upon personnel termination.
- Initial and modified access granted to IFMIS-Merger application users was not properly or timely documented and authorized.
- Documented procedures for auditing IFMIS-Merger, NDGrants, ES, EMMIE, and PARS databases, the Traverse application, and the NFIP LAN were not comprehensive and did not meet DHS requirements. Additionally, for NDGrants, ES, EMMIE, Traverse, and the NDIP LAN, logging of operating system, application, and/or database events required to be recorded was 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.
- Documented procedures for managing access to the NDGrants, ES, and EMMIE applications and databases, including sensitive access to system components managed by the FEMA IT Operations Branch System, Database and Application Management (SDAM) team, were incomplete or did not adequately consider requirements for system owner review and approval of access privileges for users and individuals with elevated privileges within the systems.
- Generic accounts and remote access to the FEN and elevated privileges to FEMA and NFIP financial systems were not authorized by the appropriate FEMA management official as required by DHS policy.
- Strong password requirements were not enforced on the NDGrants, ES, and EMMIE databases, and documentation supporting exceptions to DHS password requirements was incomplete.
- Interconnections between the FEN and one external system were not properly authorized or documented for a majority of the fiscal year.
- Documentation describing the implementation of IFMIS-Merger system user functions was incomplete or inaccurate.
- Emergency and temporary access to the IFMIS-Merger production environment was not consistently authorized.
- Certain FEMA personnel with financial reporting, management, and oversight roles were granted IFMIS-Merger application access that was excessive and/or not consistent with the principles of least

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

privilege and separation of duties, and existing system documentation did not adequately define the implementation of certain access groups and associated privileges granted to these personnel.

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

- Alternate processing sites for NDGrants, ES, and EMMIE were not established and implemented.
- Business Impact Assessments (BIAs) were not performed prior to development of the NDGrants, ES, and EMMIE CPs; FEMA management review and approval of the ES and IFMIS-Merger CPs were not performed or documented within frequencies required by DHS policy; and the EMMIE and IFMIS-Merger CPs were not updated as a result of plan testing.

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 IT security program.

For Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during our vulnerability assessments.
- Develop or revise and ensure that formal procedures are understood and consistently implemented by system owners for documenting reviews of internal vulnerability scan results, and develop and implement controls for monitoring compliance with vulnerability management policies and procedures.
- Develop or revise and implement formal configuration management plans for ES, EMMIE, and NDGrants to control 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.
- Revise formalized processes and procedures for deploying NDGrants and EMMIE changes to the production environment to ensure that the use of shared accounts for movement of production code into each production environment is appropriately authorized, controlled, and monitored.
- Develop and implement appropriate formal technical and management controls to systematically track and review modifications to the NDGrants and EMMIE production environments to ensure the completeness and integrity of change reports and logs.
- Revise and implement configuration management policies and procedures over managing configuration changes for FEN network devices supporting financial applications, including IFMIS-

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

Merger, to ensure that changes are consistently documented and authorized by FEMA management consistent with DHS policy and the FEN configuration management plan.

- Revise formal procedures for controlling changes deployed to IFMIS-Merger program libraries to reflect the current production environment, and implement controls for consistently verifying that only authorized changes are implemented into production and for retaining evidence of reviews conducted on file.
- Revise and implement comprehensive vulnerability management policies and procedures to ensure that all potential vulnerabilities identified during internal scans of the NFIP LAN supporting Traverse are documented and tracked via the POA&M process.
- Complete on-going efforts to establish and implement a separate test environment to support validation of changes to Traverse software prior to deployment to production.
- Ensure the consistent implementation of configuration management procedures and development of supporting documentation for all changes to IFMIS-Merger and TRRP.

For Security Management

- Implement policies and procedures requiring initial and periodic specialized training for individuals with significant information security responsibilities 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-Merger, FEN, EMMIE, NDGrants, and ES in accordance with DHS policy and NIST guidance, and revise and fully implement appropriate monitoring controls to ensure continued compliance with applicable criteria related to security authorization activities and supporting documentation.
- Revise and implement formalized processes to ensure that POA&Ms related to audit findings for financial systems are developed and maintained in accordance with DHS guidance.
- 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, including FEMA’s planned Operational Security (“OPSEC”) framework and associated policies, procedures, and monitoring controls, 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

- 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 the Traverse application.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

- Update, as necessary, and implement procedures and processes to ensure that all FEN 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 IFMIS-Merger, EMMIE, NDGrants, and ES database and application user accounts by system owners, 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, NDGrants, ES, EMMIE, PARS, NFIP LAN, and Traverse database, application, and operating system logs and the maintenance of documentation supporting such reviews in accordance with DHS requirements.
- Configure audit logs for NFIP LAN, Traverse, EMMIE, NDGrants, and ES databases and applications to ensure that auditable events, as required by DHS policy, are recorded, retained, and appropriately reviewed by independent security management personnel, and sufficient evidence is retained.
- Revise and implement policies and procedures for documenting, reviewing, and approving generic accounts and remote access to the FEN and elevated privileges to FEMA and NFIP financial systems, by appropriate FEMA management officials as required by DHS policy.
- Configure NDGrants, ES, and EMMIE databases to enforce strong password and authenticator control requirements for all user accounts and, if necessary and justified by operational and business requirements, ensure that documented requests for exceptions from DHS password requirements identify all affected accounts subject to deviations from standard controls.
- Revise and implement policies and procedures for documenting, reviewing, and approving external connections to the FEMA network, including documentation of roles, responsibilities, and security requirements within Interconnection Security Agreements (ISAs) or equivalent agreements.
- Revise and implement policies and procedures for documenting IFMIS-Merger security functions to ensure that system documentation accurately and completely reflects existing functionality and privileges assigned to application users.
- Implement and monitor compliance with a formal process for granting and documenting authorization of emergency and temporary access to the IFMIS-Merger production environment.
- Revise and implement controls to manage the assignment of groups and corresponding roles and functionality within the IFMIS application, including relative to individuals in financial reporting, management, or oversight roles within FEMA, by identifying conflicting roles, revising system documentation as appropriate, and modifying existing assignments to address violations of segregation of duties and least privilege principles.

For Contingency Planning

- Complete on-going efforts to establish and implement alternate processing sites for NDGrants, ES, and EMMIE.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

- Conduct and document the results of BIAs for NDGrants, ES, and EMMIE, and update corresponding CPs as appropriate based on the results of assessments.
- Update EMMIE and IFMIS-Merger CPs as appropriate based on results and lessons learned from testing, and submit ES and IFMIS-Merger CPs to appropriate FEMA management officials for review and approval at least annually.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

APPLICATION CONTROLS

We concluded that application controls over NDGrants, ES, EMMIE, IFMIS-Merger, and PARS could not be relied upon for purposes of our FY 2012 audit engagement 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, 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 financial systems during the FY 2012 FEMA audit engagement.

**Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012**

Appendix A

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

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

Below is a description of significant FEMA financial management systems and supporting IT infrastructure included in the scope of FEMA's FY 2012 financial statement 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 software package developed and maintained by Digital Systems Group Incorporated. IFMIS-Merger interfaces with PARS, ProTrac, Smartlink (Department of Health and Human Services [HHS]), Treasury Information Executive Repository (Department of the Treasury), Secure Payment System (Department of the Treasury), Grants Management System (Department of Justice), United States Coast Guard Credit Card System, Credit Card Transaction Management System (CCTMS), Fire Grants, eGrants, Enterprise Data Warehouse and Payroll (Department of Agriculture National Finance Center). The IFMIS-Merger production environment is located in Virginia.

Payment and Reporting System (PARS)

PARS is a standalone web-based application. The PARS database resides on the IFMIS-Merger UNIX server and is incorporated within the Certification & Accreditation (C&A) boundary for that system. Through its web interface, PARS collects Standard Form 425 information from grantees and stores the information in its Oracle 9i database. Automated scheduled jobs are run daily to update and interface grant and obligation information between PARS and IFMIS-Merger. All payments to grantees are made through IFMIS-Merger. PARS is located in Virginia.

Non-Disaster Grant Management System (NDGrants)

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

Emergency Support (ES)

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

In addition to IFMIS, ES has interfaces to several other FEMA systems, including:

- ISAAC (organizational and personnel data and team setup);
- Emergency Coordination (incident and disaster declarations);

**Department of Homeland Security
Federal Emergency Management Agency**
Information Technology Management Letter
September 30, 2012

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

NDGrants is located in Virginia.

Emergency Management Mission Integrated Environment (EMMIE)

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

Interfaces exist between the EMMIE system and IFMIS. EMMIE is located in Virginia.

**Department of Homeland Security
Federal Emergency Management Agency**
Information Technology Management Letter
September 30, 2012

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.

**Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012**

Appendix B

FY 2012 Notices of IT Findings and Recommendations at FEMA

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

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

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

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

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

<u>FY 2012 NFR #</u>	<u>NFR Title</u>	<u>FISCAM Control Area</u>	<u>New Issue</u>	<u>Repeat Issue</u>
FEMA-IT-12-32	Lack of EMMIE System Owner Approval for Database Accounts	Access Controls	X	
FEMA-IT-12-33	Incomplete Access Procedures for Operations Branch Database Accounts	Access Controls	X	
FEMA-IT-12-34	Lack of ES System Owner Approval for Database Accounts	Access Controls	X	
FEMA-IT-12-35	Lack of NDGrants System Owner Approval for Database Accounts	Access Controls	X	
FEMA-IT-12-36	Inconsistent Review of IFMIS-Merger Application and Database Audit Logs	Access Controls		X
FEMA-IT-12-37	Insufficient Development and Update of the EMMIE CP	Contingency Planning	X	
FEMA-IT-12-38	Non-Compliance with Alternate Processing Site Requirements for EMMIE	Contingency Planning	X	
FEMA-IT-12-39	Insufficient Review and Approval of the ES CP	Contingency Planning	X	
FEMA-IT-12-40	Non-Compliance with Alternate Processing Site Requirements for ES	Contingency Planning	X	
FEMA-IT-12-41	Incomplete POA&Ms for EMMIE SAR Weaknesses	Security Management	X	
FEMA-IT-12-42	Non-Compliant Security Authorization Package for NDGrants	Security Management	X	
FEMA-IT-12-43	Non-Compliant Security Authorization Package for ES	Security Management	X	
FEMA-IT-12-44	Incomplete Account Management Procedures for the EMMIE Application	Access Controls	X	
FEMA-IT-12-45	Incomplete Account Management Procedures for NDGrants	Access Controls	X	
FEMA-IT-12-46	Incomplete Account Management Procedures for ES	Access Controls	X	
FEMA-IT-12-47	Non-Compliance with DHS and FEMA Password Requirements for Oracle Databases Supporting Financial Applications	Access Controls	X	
FEMA-IT-12-48	Incomplete Waiver Request for Password Controls on Oracle Databases Supporting Financial Applications	Access Controls	X	
FEMA-IT-12-49	Inconsistent Authorization of Temporary Access to IFMIS-Merger System Software	Access Controls and Configuration Management		X

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012

<u>FY 2012 NFR #</u>	<u>NFR Title</u>	<u>FISCAM Control Area</u>	<u>New Issue</u>	<u>Repeat Issue</u>
FEMA-IT-12-50	Inadequate Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment	Configuration Management		X
FEMA-IT-12-51	Inconsistent Activities and Incomplete Documentation Supporting Configuration Changes for the IFMIS-Merger Application	Configuration Management	X	
FEMA-IT-12-52	Lack of ES Information System Security Officer Review of Monthly Vulnerability Scan Results	Configuration Management	X	
FEMA-IT-12-53	Insufficient Audit Log Controls for EMMIE	Access Controls	X	
FEMA-IT-12-54	Insufficient Audit Log Controls for NDGrants	Access Controls	X	
FEMA-IT-12-55	Insufficient Audit Log Controls for ES	Access Controls	X	
FEMA-IT-12-56	Incomplete Documentation Supporting EMMIE Configuration Management Controls	Configuration Management	X	
FEMA-IT-12-57	Unauthorized Shared Account Usage for EMMIE and NDGrants Production Application Deployments	Configuration Management	X	
FEMA-IT-12-58	Lack of Controls to Validate Completeness and Integrity of EMMIE and NDGrants Application Changes Deployed to Production	Configuration Management	X	
FEMA-IT-12-59	Incomplete Documentation Supporting NDGrants Configuration Management Controls	Configuration Management	X	
FEMA-IT-12-60	Incomplete Vulnerability Management Procedures	Configuration Management	X	
FEMA-IT-12-61	Excessive or Inappropriate Access to IFMIS	Access Controls	X	

**Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012**

Appendix C

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

**Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012**

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-01	Alternate Processing Site for NEMIS Has Not Been Established	X	
FEMA-IT-11-02	Weaknesses Exist in the C&A Package for the FEMA Switched Network (FSN)-2, which Includes the FEMA LAN		FEMA-IT-12-21
FEMA-IT-11-03	Weaknesses Exist over the ATO and C&A Documentation for NEMIS	X	
FEMA-IT-11-04	NEMIS CP Does Not Comprehensively Address the Requirements of DHS Policy and Has Not Been Adequately Tested	X	
FEMA-IT-11-05	Formalized Training Requirements for Individuals with Significant Information Security Responsibilities Have Not Been Fully Implemented and Role-Based Training is Not Tracked or Monitored		FEMA-IT-12-13
FEMA-IT-11-06	Documentation Supporting IFMIS-Merger User Functions Does Not Exist		FEMA-IT-12-04
FEMA-IT-11-07	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary are Not Configured to Enforce Password Requirements	X	
FEMA-IT-11-08	Oracle Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary Do Not Adequately Enforce Account Lockout Requirements	X	
FEMA-IT-11-09	Operating System Audit Logging on Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate	X	
FEMA-IT-11-10	Weaknesses Existed over Contingency Planning, Testing and Development of the Continuity of Operations Plan for TRRP and Traverse	X	
FEMA-IT-11-11	Recertification of NEMIS Access Control System Position Assignments is Incomplete	X	
FEMA-IT-11-12	Audit Logging on Databases Supporting Financial Applications within the Previous NEMIS Accreditation Boundary is Not Adequate	X	
FEMA-IT-11-13	Weaknesses Exist over Vulnerability Management for Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary	X	
FEMA-IT-11-14	NFIP Physical Access Policies and Procedures were Not Appropriately Documented and Implemented	X	
FEMA-IT-11-15	NFIP LAN and Traverse Account Security Configuration Is Not in Compliance with DHS Policy	X	

**Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012**

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-16	TRRP Logical Access was Not Appropriately Authorized	X	
FEMA-IT-11-17	Weaknesses Exist over Configuration and Operating Effectiveness of Traverse Audit Logs		FEMA-IT-12-02
FEMA-IT-11-18	Inadequate Monitoring of Configuration Changes Deployed to the IFMIS-Merger Production Environment		FEMA-IT-12-50
FEMA-IT-11-19	Weaknesses Exist over Configuration Management Processes for Financial Applications within the Previous NEMIS Accreditation Boundary	X	
FEMA-IT-11-20	Weaknesses Exist over IFMIS-Merger Configuration Management Processes	X	
FEMA-IT-11-21	Weaknesses Exist over Recertification of Access to the IFMIS-Merger Application	X	
FEMA-IT-11-22	Weaknesses Exist over TRRP Mainframe Audit Logs	X	
FEMA-IT-11-23	Emergency and Temporary Access to IFMIS-Merger is Not Properly Authorized		FEMA-IT-12-49
FEMA-IT-11-24	Weaknesses Exist over IFMIS-Merger Application and Database Audit Logging		FEMA-IT-12-36
FEMA-IT-11-25	IFMIS–Merger User Access was Not Managed in Accordance with Account Management Procedures	X	
FEMA-IT-11-26	PARS Database Security Controls Are Not Appropriately Established	X	
FEMA-IT-11-27	NFIP LAN Audit Logging is Not Performed in Accordance with DHS and FEMA Requirements		FEMA-IT-12-03
FEMA-IT-11-28	Individual User Virtual Private Network (VPN) Access Accounts are Not Appropriately Authorized or Recertified	X	
FEMA-IT-11-29	External Connections to the FEMA VPN Are Not Appropriately Authorized or Documented	X	
FEMA-IT-11-30	IFMIS-Merger System Software Administrator Activity Is Not Appropriately Restricted or Monitored	X	
FEMA-IT-11-31	Weaknesses Exist over C&A Documentation for IFMIS-Merger	X	
FEMA-IT-11-32	Risk Assessment Activities over NFIP IT Systems were Not Adequately Performed	X	
FEMA-IT-11-33	Weaknesses Exist over Management and Technical Controls Associated with FEMA LAN Accounts		FEMA-IT-12-12
FEMA-IT-11-34	Employee Termination Process for Removing System Access Should Be More Proactive	X	

**Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2012**

NFR #	Description	Disposition	
		Closed	Repeat
FEMA-IT-11-35	Traverse Configuration Management Plan Weaknesses		FEMA-IT-12-23
FEMA-IT-11-36	TRRP Configuration Management Plan Weaknesses		FEMA-IT-12-24
FEMA-IT-11-37	Documentation Supporting TRRP Test Libraries Does Not Reflect Current Environment	X	
FEMA-IT-11-38	Federal Insurance and Mitigation Administration CMP has Not Been Developed	X	
FEMA-IT-11-39	Weaknesses Exist over Background Investigations for Federal Employees and Contractors		FEMA-IT-12-28
FEMA-IT-11-40	Weaknesses in the Management of POA&Ms for Audit Findings over FEMA Financial Systems		FEMA-IT-12-15
FEMA-IT-11-41	Physical Security and Security Awareness Issues Associated with Enhanced Security Testing at FEMA		FEMA-IT-12-01
FEMA-IT-11-42	Traverse Accounts Were Not Appropriately Recertified	X	
FEMA-IT-11-43	Lack of Adequate Configuration Management over Network Devices Supporting Financial Systems		FEMA-IT-12-17
FEMA-IT-11-44	Password, Patch, and Configuration Management Weaknesses Were Identified during the Vulnerability Assessment on IFMIS, NEMIS, and Key Support Servers		FEMA-IT-12-06
FEMA-IT-11-45	Vulnerability Assessment Program for the NFIP LAN Supporting Traverse was Inadequate	X	
FEMA-IT-11-46	Weaknesses Existed over the Configuration Patch Management Process for the NFIP LAN Supporting Traverse	X	
FEMA-IT-11-47	Weaknesses Exist over the Configuration and Testing of Backups for Servers Supporting Financial Applications within the Previous NEMIS Accreditation Boundary	X	
FEMA-IT-11-48	Key Controls over Production Servers Supporting Applications within the Former NEMIS Accreditation Boundary Have Not Been Implemented	X	

ADDITIONAL INFORMATION AND COPIES

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

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

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

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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