Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY2010 DHS Financial Statement Audit

OIG-11-79

May 2011

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

MAY 06 2011

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 DHS financial statement audit as of September 30, 2010. It contains observations and recommendations related to IT internal control that were summarized in the *Independent Auditor's Report* dated November 12, 2010 and presents 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 2010 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 22, 2011, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

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

Frank Deffer
Assistant Inspector General
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

March 22, 2011

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
Federal Emergency Management Agency

Ladies and Gentlemen:

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS or Department), as of September 30, 2010 and the related statement of custodial activity for the year then ended (herein after referred to as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2010 and the statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources as of September 30, 2010 (hereinafter referred to as "other fiscal year (FY) 2010 financial statements"), or to examine internal control over financial reporting over the other FY 2010 financial statements.

Because of matters discussed in our *Independent Auditors' Report,* dated November 12, 2010, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and the related statement of custodial activity for the year then ended. Additional deficiencies in internal control over financial reporting, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and the related statement of custodial activity for the year then ended; and had we been engaged to audit the other FY 2010 financial statements, and to examine internal control over financial reporting over the other FY 2010 financial statements.

A control deficiency 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 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. A material weakness is a deficiency, or a 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.

The Federal Emergency Management Agency (FEMA) is a component of DHS. During our audit engagement, we noted certain matters in the areas of information technology (IT) configuration management, security management, access controls, segregation of duties, and contingency planning with respect to FEMA's financial systems IT general controls, which we believe collectively contribute to an IT material weakness at the DHS level. These matters are described in the *IT General Control Findings and Recommendations* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 12, 2010. This letter represents the separate limited distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through Notices of Finding and Recommendation (NFR).

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. We aim to use our knowledge of FEMA gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies. 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 and IT infrastructure within the scope of our engagement to audit the FY 2010 DHS financial statements 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 certain additional matters have been presented in a separate letter to the Office of Inspector General and the FEMA Chief Financial Officer.

FEMA's written response to our comments and recommendations, presented in Appendix D, has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of DHS and FEMA management, DHS Office of Inspector General, U.S. Office of Management and Budget, U.S. Government Accountability Office, 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, 2010

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

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

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit the Department of Homeland Security's (DHS or department) balance sheet as of September 30, 2010 and the related statement of custodial activity for the year then ended, we performed an evaluation of information technology general controls (ITGC) at the Federal Emergency Management Agency (FEMA), to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our ITGC evaluation procedures. The scope of the ITGC 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 general IT controls environment:

- *Security Management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access Control (AC)* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and 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 general IT controls 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.

Additionally, during FY 2009, we were informed by FEMA management that the Grants & Training (G&T) Integrated Financial Management Information System (IFMIS) and Core IFMIS versions would be merged into one system. Between October 1, 2009 and February 22, 2010, G&T and Core IFMIS were both operational and used to process FEMA financial data. As a result, we performed testing for both the Core and G&T IFMIS versions.

On February 23, 2010, FEMA suspended the use of the G&T IFMIS version and had completed the final changes to Core IFMIS which would then become IFMIS-Merger. We were informed that the final IFMIS-Merger version went live on February 23, 2010 and is now the system of record. Therefore, for the purposes of this letter, the audit testwork conducted over general controls and weaknesses identified for Core IFMIS are reported as part of controls over IFMIS-Merger.

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) 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 fiscal year (FY) 2010, FEMA took corrective action to address certain prior year IT control weaknesses. For example, FEMA made improvements over implementing certain logical and physical access controls over NFIP information systems, as well as development and maintenance of the inventory of FEMA Chief Financial Officer (CFO)-designed financial management systems. However, during FY 2010, we continued to identify ITGC 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 IFMIS-Merger, G&T IFMIS, the National Emergency Management Information System (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 ITGC 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 63 findings identified during our FY 2010 testing, 50 were repeat findings, either partially or in whole from the prior year, and 13 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.

IT GENERAL CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2010 DHS financial statement audit engagement, we identified the following financial system ITGC 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:

- Documented and approved procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of NEMIS, IFMIS-Merger and G&T IFMIS had not been developed and implemented. Additionally, during periodic internal scans, vulnerabilities identified and related corrective actions were not reported and tracked via the Plan Of Action &Milestones (POA&M) process in accordance with DHS policy.
- Formal procedures for conducting internal scans of the NFIP Local Area Network (LAN) supporting Traverse were not developed, and scans were not conducted 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 list of NEMIS servers currently scanned internally by FEMA is incomplete and does not represent the current NEMIS system boundary. Additionally, NEMIS system owners are not receiving listings of all vulnerabilities noted on their system components to ensure corrective action is assigned for tracking and remediation.
- The Standard Operating Procedure (SOP) for monitoring sensitive access to NEMIS operating system software was not implemented and did not include all NEMIS operating system servers that were within scope. Additionally, no application or tool was in place to support the audit logging function on the NEMIS servers.
- NEMIS configuration management is not adequately and centrally controlled, documented, or managed throughout the lifecycle of the FEMA configuration management process. Additionally, implemented emergency and non-emergency changes to NEMIS system software were not consistently documented, tested, approved, controlled, tracked, and retained on file.
- No formalized change management procedures exist for deploying changes to the NEMIS production environment to ensure that the movement of production code for NEMIS is appropriately controlled. 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.
- G&T IFMIS contracted developers/programmers were granted unrestricted access to the production environment through the "ifmiscm" account, which was used to deploy changes into production.

- Comprehensive configuration baselines for all relevant network devices such as firewalls, routers, and switches that support in-scope financial systems had not been established. Furthermore, configuration management policies and procedures did not include comprehensive requirements for the frequency, documentation and performance of monitoring audits for these baselines to ensure that configuration items (CIs) within the scope of the IFMIS-Merger and NEMIS systems are documented and monitored in accordance with FEMA policy.
- Adequate segregation of duties controls had not been established for the movement of IFMIS-Merger changes into production as the IFMIS-Merger developer migrates changes into production. Additionally, formal procedures were not implemented to require monitoring of developers' changes to IFMIS-Merger directories and sub-directories 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.
- Throughout the lifecycle of the project to merge G&T IFMIS and Core IFMIS to IFMIS-Merger, FEMA management did not adequately define, implement, and integrate the required elements of the DHS System Engineering Life Cycle (SELC) process. We noted that the project lacked defined project review stages and approvals, system security requirements and milestones were not documented and integrated into the project plan, and a Data Migration Plan and Testing Strategy could not be provided.
- The configuration management plans for IFMIS-Merger, 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.
- Formal patch management procedures for approving, testing, and ensuring timely installation of operating system patches for NEMIS, IFMIS-Merger, and G&T IFMIS were not developed and finalized until April 2010. Additionally, FEMA had not fully and consistently implemented the requirements and procedures documented.
- Documented change management procedures did not include requirements for approving, testing, and ensuring timely installation of operating system patches for the NFIP LAN supporting Traverse.
- The third-party development vendor was allowed use of NFIP system administrator accounts to logon and create sessions for installing Traverse system changes, and a formal process was not established for monitoring changes made by the vendor.

Security Management:

- Policies and procedures requiring the completion and tracking of specialized training for FEMA employees and contractors with significant information security responsibilities had not been established or implemented as required by DHS policy. Additionally, with the exception of Information System Security Officers (ISSOs), FEMA had not formally identified all individuals or positions that were subject to the training requirements.

- G&T IFMIS was not certified and accredited prior to implementation into the production environment in FY 2007 and had been operating without an Authorization to Operate (ATO) for the majority of FY 2010.
- Web and application servers for PARS had not been certified and accredited, and the PARS database operated for the majority of FY 2010 without an adequate ATO.
- ISSOs were not formally designated for G&T IFMIS and PARS for the majority of the fiscal year.
- Certification and accreditation (C&A) activities for IFMIS-Merger and NEMIS 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 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.
- The system security plan (SSP) for NEMIS did not fully document the systems boundaries, define all subsystems and major applications, or document the assignment of FEMA personnel with security responsibilities for all system components.
- The C&A for the legacy NFIP IT system pertaining to the Traverse application, TRRP application, and NFIP LAN had not been certified and accredited or fully authorized for operation, in accordance with DHS policy for FY 2010.
- Procedures for managing FEMA IT security incidents were not developed, approved, and implemented, in accordance with DHS policy.
- Entity-level corrective actions to integrate and develop sufficient and effective methods of communication to ensure that significant financial-related system development and acquisition projects involve all relevant stakeholders, including the Office of the Chief Financial Officer (OCFO), had not been established. Additionally, FEMA management had not taken action to enhance and further develop current acquisition management processes to ensure that organization-specific requirements exist and are implemented so that each project meets organizational mission needs and functional and technical requirements as required by DHS and NIST guidance.
- IT security management responsibilities were not consistently or adequately assigned and performed over the FEMA POA&M process for FY 2009 IT audit findings, in accordance with DHS guidance.
- Suitability investigations for FEMA federal employees and contractors were not appropriately conducted, and position sensitivity levels associated with employees and contractors with elevated system privileges did not have appropriate position sensitivity designations. Additionally, formal procedures were not developed or implemented for conducting suitability screenings for contractors accessing DHS IT systems.

- FEMA did not have a process for centrally tracking the status of contractors or an effective and formal process for notifying the Office of the Chief Information Officer (OCIO) of changes in contractor status so that contractor user accounts could be appropriately disabled, removed, or modified in a timely manner.

Related to security management, 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	TechWorld	
Passwords	5	3	3	**11**
For Official Use Only (FOUO)	0	1	0	**1**
Keys	0	0	0	**0**
Personally Identifiable Information (PII)	3	2	3	**8**
External Drives	0	0	1	**1**
Server Names/ IP Addresses	2	2	0	**4**
Credit Card Numbers	0	1	1	**2**
Classified Documents	0	0	0	**0**
Other	1	2	3	**6**
Total by Location	**11**	**11**	**11**	**33**

To complement FY 2010 security management audit procedures, social engineering testing was conducted. 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, several personnel provided us with user IDs and/or passwords. The specific results of our testing are documented in the table below:

Testing Date	Total Called	Total Answered	# of Personnel Who Provided Their User ID and Password	# of Personnel Who Provided Their User ID Only	# of Personnel Who Provided Their Password Only
07/08/2010	25	11	2	4	0
08/11/2010	34	11	1	8	1

Access controls:

- Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting the key financial applications and general support systems.
- TRRP, IFMIS-Merger, G&T IFMIS, NEMIS, 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. For G&T IFMIS, we determined that recertification of user accounts had not been conducted since the application was implemented at FEMA in FY 2007.
- IFMIS-Merger, G&T IFMIS, 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 IFMIS-Merger, G&T IFMIS and PARS financial application and/or database, network, and remote users was not properly documented and authorized.
- Documented procedures for auditing NEMIS, IFMIS-Merger, G&T IFMIS, and PARS databases were not comprehensive and did not meet DHS requirements. Additionally, for these financial systems and the NFIP LAN 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.
- Strong password requirements were not enforced on the NEMIS, IFMIS-Merger, G&T IFMIS, and PARS databases and the FEMA LAN.
- 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.
- A formalized process for modifying IFMIS-Merger system security functions to ensure that appropriate privileges are created, documented, approved, and monitored did not exist.
- Two-factor authentication was not used for VPN access, as required by DHS policy.
- System administrator root access to IFMIS-Merger and G&T IFMIS were not properly restricted, logged, and monitored.
- Emergency and temporary access to the IFMIS-Merger and G&T IFMIS databases was not properly authorized, and contractor development personnel were granted conflicting access to implement database changes.

Segregation of Duties:

- Access was inappropriately granted to NEMIS developers to allow unrestricted access to both the production and development code in the Test and Development Laboratory (TDL) environment, and NEMIS code approved for implementation was not locked down within the TDL environment prior to deployment to production to further restrict developer access.
- Additional segregation of duties weaknesses were noted in 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:

- 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.
- 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. Additionally, evidence that all databases were being backed up could not be provided.
- NEMIS backup tapes were not regularly tested in accordance with FEMA and DHS policy.
- Full scale testing of the NEMIS contingency plan was not conducted, and the plan did not adequately and comprehensively include information for fully restoring NEMIS in accordance with requirements for high impact availability systems or accurately include NEMIS system architecture information.
- The existing NFIP LAN and Traverse contingency plan was not updated and in compliance with DHS and NIST requirements. Additionally, the plan had not been tested within the past 12 months, and no alternate processing site had been identified.
- A documented and approved IT contingency plan for the mainframe environment supporting the TRRP system has not been completed, and contingency testing over TRRP was not sufficiently conducted in accordance with DHS and NIST requirements.
- The NFIP contractor's Continuity of Operations Planning (COOP) for Traverse and TRRP could not be provided for auditor review.

Recommendations:

No recommendations are required for the G&T IFMIS portions of the conditions noted above as the system was decommissioned in June 2010. 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:

- Develop, finalize, and implement formal procedures over NEMIS and IFMIS-Merger operating systems and the NFIP LAN supporting Traverse for: (1) conducting periodic internal vulnerability scans of FEMA and NFIP financial systems; (2) assessing, reporting, tracking, and monitoring correcting vulnerabilities identified during internal scans; and (3) ensuring procedures are implemented for all components of the systems;
- 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;
- Develop and implement configuration management policies and procedures for NEMIS 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 the movement of production code for the NEMIS production environment is appropriately controlled;
- Revise and implement configuration management policies and procedures over documenting and maintaining current baseline configurations for network devices supporting financial applications, including IFMIS-Merger and NEMIS, to ensure DHS and FEMA requirements are adequately addressed and configuration baselines are comprehensively documented 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;
- Limit IFMIS-Merger developer access to the production environment to "read only," and segregate the responsibility for deploying application code changes into production from the development contractor to an independent control group. If business needs require that the segregation of duties cannot be immediately implemented, develop and implement formal procedures for conducting periodic reviews of IFMIS-Merger developer changes to financial application directories and sub-directories to verify that only authorized changes are implemented into production and for retaining evidence of reviews conducted on file;
- Conduct and document a lessons learned report related to the IFMIS-Merger project per DHS SELC guidance;
- Update the current versions of IFMIS-Merger, Traverse, and TRRP configuration management plans and procedures to comprehensively address DHS and FEMA requirements. Additionally, ensure the implementation of updated versions of the current IFMIS-Merger, Traverse, and TRRP configuration management procedures. The procedures should require initial approvals of change requests and establish a process for obtaining Change Control Board and Technical Review Committee approvals prior to implementing standard and emergency changes into production;

- Dedicate the appropriate resources to complete efforts to further document and fully implement comprehensive patch management policies and procedures for NEMIS and IFMIS-Merger;
- Document, finalize, and implement comprehensive patch management policies and procedures that outline requirements for authorizing, testing, and installing required patches for the NFIP LAN operating system supporting Traverse; and
- Limit Traverse development vendor access to the production environment to "read only," and segregate the responsibility for deploying application code changes into production from the development contractor to an independent control group. If business needs require that the segregation of duties cannot be immediately implemented, establish a separate account for use by the NFIP third-party development vendor when implementing Traverse changes that is limited to activation on an as-needed basis, and establish a process for monitoring and verifying that configuration changes by the vendor are implemented and documented in accordance with policy.

For Security Management:

- Develop and implement policies and procedures requiring initial and periodic specialized training for individuals with significant information security responsibilities. Policies and procedures should identify specific roles and positions possessing significant information security responsibilities that are subject to specialized training requirements and include requirements for tracking training;
- Certify and accredit all components of PARS in accordance with applicable DHS policies and Federal guidance, and formally designate an ISSO for all components of the system;
- Update and complete 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;
- Ensure that the NEMIS SSP is updated in accordance with DHS policy so that the system's boundaries, components, and roles and responsibilities are properly defined and documented. Additionally, implement a formal process for periodically reviewing and assessing system documentation to ensure software and hardware components are accurately reflected;
- Develop and implement approved procedures for managing security incidents that clearly outline roles and responsibilities required to maintain a continuous incident response capability, and provide training to all personnel with assigned roles and responsibilities;
- Define and implement formal and repeatable processes to ensure that financial systems development and acquisition projects are conducted in compliance with DHS SELC and acquisition requirements and Federal guidance;

- 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 performed, and reevaluate and assign the correct position sensitivity levels for federal employees and contractors with access to DHS information systems. FEMA Acquisitions, FEMA Personnel Security, and FEMA IT should also work together to implement procedures to ensure a more centralized and coordinated process for tracking and completing background investigations over contractor personnel, in accordance with DHS policy;
- Document and implement procedures for tracking contractor on-boards, transfers, and separations that include assignment of roles and responsibilities to appropriate FEMA management and stakeholders and steps for notifying the OCIO and system owners of changes in contractor status that require changes to user access; and
- 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:

- 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;
- 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 on IFMIS-Merger, NEMIS, TRRP, and PARS as well as the FEMA/NFIP networks and remote user accounts. The processes should include revocation of accounts 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, and PARS database and financial application logs and the maintenance of documentation supporting such reviews in accordance with DHS requirement. 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;
- Configure NEMIS, IFMIS-Merger, and PARS databases and FEMA LAN 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;
- 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;
- Implement and require two-factor authentication for all remote access to the FEMA network;
- 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
- Establish 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 Segregation of Duties:

- Develop and implement formal processes and procedures for restricting and monitoring access to the NEMIS TDL directories to ensure that the principles of least privilege and segregation of duties are enforced. The processes should include requirements over the monitoring of NEMIS TDL directories to ensure that no changes have occurred after the approval of NEMIS system changes has occurred and should limit developers' access to the approved code for production to "read only."

For Contingency Planning:

- Complete on-going efforts to establish and implement an alternate processing site for NEMIS;
- Ensure that a formal process is established and implemented to fully backup all necessary components of the NEMIS database and periodically test NEMIS backup media at a frequency that is in accordance with FEMA and DHS policy;
- 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;

- Update and appropriately test the NFIP contingency plan pertaining to the NFIP LAN and Traverse system, in accordance with DHS requirements; identify alternate processing sites for each system; and test fail-over capability at the alternate processing site;
- Develop, document, and fully implement an IT contingency plan for TRRP in accordance with DHS requirements; conduct documented annual tests of the plan; and as necessary, update the plan with lessons learned from testing; and
- Document, implement, and maintain the NFIP COOP to ensure required elements for Traverse and TRRP are included in accordance with DHS guidance for high impact systems.

APPLICATION CONTROLS

We concluded that application controls over NEMIS, IFMIS-Merger, G&T IFMIS, and PARS could not be relied upon for purposes of our FY 2010 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 2010 DHS financial statement audit engagement.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We received written comments on a draft of this report from FEMA's Chief Information Officer. Generally, FEMA agreed with our findings and recommendations. FEMA's management has developed a remediation plan to address these findings and recommendations. A copy of the comments is included in Appendix D.

OIG Response

We agree with the steps that FEMA's management is taking to satisfy these recommendations.

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

Appendix A

Description of Key Federal Emergency Management Agency Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit Engagement

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

Below is a description of significant FEMA financial management systems and supporting IT infrastructure included in the scope of the DHS FY 2010 financial statement audit engagement.

Locations of Testing FEMA Headquarters in Washington, D.C.; the Mount Weather Emergency Operations Center in Bluemont, Virginia; IT operations in Winchester, Virginia; NFIP in Crystal City, Virginia; and the NFIP contractor location in Lanham, Maryland (which was later moved in August 2010 to Landover, Maryland).

Systems Subject to Audit:

Core Integrated Financial Management Information System (IFMIS)[1] *(Operational through February 22, 2010)* Core IFMIS was the key financial reporting system and had several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting). The application was a Commercial Off-The Shelf (COTS) software package developed and maintained by Digital Systems Group Incorporated (DSG).

Grants and Training (G&T) IFMIS[2] *(Operational through February 22, 2010)* In April 2007, the Office of G&T that was previously under the Department of Justice was transferred to FEMA. Due to the short amount of time given to FEMA to take over the financial management role for G&T in FY 2007, a separate instance of IFMIS was inherited from the Department of Justice, resulting in two separate IFMIS instances at FEMA. G&T IFMIS held all former G&T financial information. The application was a COTS software package developed and maintained by DSG.

IFMIS-Merger[3] *(Operational beginning February 23, 2010)* 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 COTS software package developed and maintained by DSG.

[1] During FY 2009, FEMA management reported that the G&T IFMIS and Core IFMIS versions would be merged into one system. Between October 1, 2009 and February 22, 2010, G&T and Core IFMIS were both operational and used to process FEMA financial data. On February 23, 2010, FEMA suspended the use of the G&T IFMIS version and had completed the final changes to Core IFMIS which would then become IFMIS-Merger. The final IFMIS-Merger version went live on February 23, 2010 and is now the system of record.
[2] G&T IFMIS was decommissioned in June 2010 after the merger of G&T IFMIS and Core IFMIS in February 2010.
[3] On February 23, 2010, the final IFMIS-Merger version went live on February 23, 2010 and is now the system of record.

Payment and Reporting System (PARS)

PARS is a standalone web-based application. The PARS database resides on the IFMIS-Merger UNIX server[4]. Through its web interface, PARS collects Standard Form 425 (SF-425) information from grantees and stores the information in its Oracle 9i database. Automated chronologic 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. Prior to the IFMIS-Merger instance in February 2010, the PARS application interfaced with G&T IFMIS.

National Emergency Management Information System (NEMIS)

NEMIS is a FEMA-wide system of hardware, software, telecommunications, 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 automation to perform disaster related operations. NEMIS supports all phases of emergency management and provides financial related data to IFMIS via an automated interface.

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 in Landover, Maryland (previously Lanham, Maryland). The Traverse client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members.

Transaction Recording and Reporting Processing (TRRP)

The TRRP application acts as a central repository of all data submitted by the Write Your Own (WYO) companies for the NFIP. TRRP also supports the WYO program, primarily by ensuring the quality of financial data submitted by the WYO companies to TRRP. TRRP is a mainframe-based application that runs on the NFIP mainframe logical partition in Norwich, Connecticut.

[4] Prior to the merger of Core IFMIS and G&T IFMIS, PARS resided on the Core IFMIS server.

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

Appendix B

FY 2010 Notices of IT Findings and Recommendations at the Federal Emergency Management Agency

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

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 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 FEMA in the development of its corrective action plans for remediation of each deficiency.

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

Notice of Findings and Recommendations – Detail

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-01	During FY 2010, FEMA finalized and documented requirements, and initiated automated technical processes and controls related to the NEMIS Access Control System (NACS) Position Re-Approval Project (NPRP). Specifically, Enterprise Operations Branch personnel have begun systematically expiring position assignments and requiring supervisor reauthorization of a subset of NACS accounts and related positions progressively over a 180 day period. Due to the volume of active positions, FEMA management stated that the recertification process will recertify all NACS positions after the 180 days and is anticipated to be completed in FY 2011. Thus, while we noted that improvements were made by developing and implementing an automated process for recertifying all NACS accounts and related positions, including those related to NEMIS access, initial recertification to review and revalidate all NACS accounts and positions has still not been completed.	• Complete the initial recertification of all existing NACS accounts and related positions initiated in April 2010 to ensure that all active NEMIS accounts and their associated privileges are appropriately authorized; and • Ensure that all NACS accounts and related positions are recertified by the user's appropriate supervisor no less than annually, in accordance with DHS policy.		X	3
FEMA-IT-10-02	FEMA has not established an alternate processing site for NEMIS. 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, has not been requested by FEMA.	• Continue and complete efforts required to establish and implement an alternate processing site for NEMIS according to DHS 4300A. • Until an alternate processing site is established, develop and submit an exception for approval in accordance with DHS policy, and ensure that compensating controls over the alternate processing site have been implemented and are effective, and documentation of their effectiveness is maintained as auditable records.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-03	The FEMA domain security policy is configured to enforce activation of a password-protected screensaver on end-user workstations after 15 minutes of inactivity, rather than the five minute inactivity threshold required by DHS policy.	• Configure the FEMA LAN domain security policy to automatically activate a password-protected screensaver on end-user workstations after five minutes of inactivity, consistent with DHS policy. • Implement appropriate management controls to ensure timely communication and implementation of existing and future DHS information security policy requirements pertaining to the configuration of FEMA end user workstations, and to periodically assess system controls to determine compliance.		X	2
FEMA-IT-10-04	As noted during our FY 2009 audit procedures, weaknesses exist in processes related to logging, monitoring, and retaining audit logs on system software and operating systems supporting NEMIS. Specifically, policies and procedures related to the monitoring of activity on system software and operating systems supporting NEMIS have not been revised to include all identified operating systems and IT components that comprise the system boundary for the NEMIS application. Additionally, controls have not been configured and appropriately implemented to log, monitor, or retain sufficiently detailed audit logs for activity on NEMIS operating systems and servers.	• Revise the SOP, *Monitoring Sensitive Access to NEMIS*, to ensure that it states that the scope of the procedures includes operating systems on all servers within system boundaries as defined in up-to-date NEMIS system documentation. • Acquire and deploy appropriate tools on operating systems and servers supporting NEMIS to generate audit trails and records in accordance with FEMA and DHS policy. • Implement the SOP, *Monitoring Sensitive Access to NEMIS*, by reviewing and retaining audit trails and records in accordance with FEMA and DHS policy.		X	3
FEMA-IT-10-05	As identified during the FY 2009 audit engagement, PARS database security controls are not appropriately established as noted below: • PARS database accounts are not reviewed to identify	• Document and implement a formal process to implement appropriate controls to ensure that inactive PARS database accounts are disabled in accordance with DHS policy.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	accounts that have been inactive for 45 days or more, as required by DHS policy for high impact systems.
	• Strong passwords and authenticator controls are not implemented for PARS database accounts in accordance with FEMA and DHS policy. Specifically:
	  • A minimum password length is not set;
	  • Password complexity is not enforced to require passwords that include a combination of upper/lowercase letters, numbers, and special characters or to restrict the use of dictionary words as passwords;
	  • Reuse of previous passwords is not prohibited;
	  • Passwords are not configured to expire or be changed after a pre-determined length of time; and
	  • Accounts are not configured to disable after a pre-determined number of consecutive invalid login attempts.
	• System-specific policies and procedures have not been developed for the PARS Oracle database, and existing policies and procedures inherited from the IFMIS application operating environment do not adequately describe implementation of FEMA policies for the generation, review, and retention of all required auditable events.
	• Database audit logs are not configured to capture auditable events, including failed login attempts and
		• Configure PARS database accounts in accordance with DHS and FEMA requirements for passwords and authenticator controls, including expiration, reuse, and complexity.
		• Document and implement system-specific processes for generating and performing reviews of PARS database audit logs and retaining auditable evidence of review in accordance with FEMA and DHS policy. Additionally, ensure that all DHS requirements are met through this process, including appropriate supervisory review and segregation of duties principles.
		• Configure PARS database audit logs to capture and retain auditable events in accordance with FEMA and DHS policy.
		• Further define and establish a formal process for granting initial access and recertifying access specifically to the PARS database that includes appropriate approval from FEMA management and requirements for temporary and emergency access, in accordance with DHS guidance.
		
		Please see NFR FEMA-IT-10-48 for recommendations related to the periodic review and assessment of security controls in place to ensure that corrective actions are appropriately implemented over identified security weaknesses.			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	administrator-level actions, as required by FEMA and DHS policy.
	• Although a periodic recertification of PARS database access accounts is performed to ensure that access is still necessary and appropriate for each individual, policies and procedures over the management of accounts on the PARS Oracle database do not specify requirements for performing a periodic recertification of database accounts to validate the continued appropriateness of access. Additionally, the FY 2010 recertification of PARS Oracle database user accounts was not completed consistently and in accordance with FEMA requirements. Specifically, of a selection of recertification forms for five PARS database user accounts requested, four forms recertified access for contractors without documented Contracting Officer's Technical Representative (COTR) approval.
	• Authorization of initial access for the PARS database is not consistently completed in accordance with FEMA and DHS policy. Specifically, of a selection of three PARS database access forms requested:
	  • Two user accounts were granted to contractors without the required COTR signature.
	  • One account was identified by Financial Systems Section (FSS) personnel as an IFMIS system account. However, no documentation justifying or authorizing the use of this system account was provided.				

FEMA-IT-10-06	During the FY 2010 audit engagement, we noted that FEMA has made improvements over the management of	Configure all NEMIS Oracle databases to ensure compliance with effective DHS and FEMA policy		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	NEMIS Oracle database password controls for IT Operations database administrator accounts, specifically by configuring a 104-day password lifetime. However, the following weaknesses noted in FY 2009 continue to exist in FY 2010 for the four databases selected for testing: • A password complexity verification function is not configured to require a combination of upper/lowercase letters, numbers, and special characters. • Reuse of previous passwords is not prohibited. • No minimum password length is enforced.	requirements for passwords and authenticator control requirements, including expiration, reuse, length and complexity.			
FEMA-IT-10-07	FEMA has made improvements over the management of IFMIS-Merger Oracle database passwords by configuring the system to retain a history of the previous ten passwords. However, upon inspection of additional database password parameters, we determined that the password history for the ten previous passwords is only retained for 30 days. Therefore, after the 30 day timeframe, the password history is erased, allowing the user to potentially use one of the previous ten passwords.	Configure the IFMIS-Merger Oracle database to ensure compliance with effective DHS and FEMA policy requirements regarding the reuse of user passwords.		X	3
FEMA-IT-10-08	During the FY 2010 audit engagement, we selected four NEMIS Oracle databases for testing and noted that each is configured to lock accounts after three consecutive failed login attempts and to remain locked for 415 seconds (7.5 minutes) before being unlocked.	Configure all NEMIS Oracle databases to ensure compliance with effective DHS and FEMA policy requirements for account lockouts due to failed login attempts.	X		3
FEMA-IT-10-09	As noted during the FY 2009 audit engagement, the following weaknesses over audit logging controls for the NEMIS Oracle databases continue to exist in FY 2010:	• Revise the *SOP for Handling of Oracle Audit Logs* to ensure that procedures over requirements for logging and monitoring auditable activities on		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	• The FEMA IT Operations Branch *Standard Operating Procedure (SOP) for Handling of Oracle Audit Logs* has not been updated. Specifically:
	  • The scope section of the SOP does not list all Oracle databases identified that comprise the NEMIS data processing environment.
	  • The SOP has not been updated to address all DHS policy requirements surrounding audit trails and activity monitoring. Specifically, successful logins, access modifications, highly privileged user account activity, and changes to user profiles are not required to be logged and reviewed.
	  • The SOP specifies that database administrators will review Oracle audit records, which is a violation of segregation of duties principles that require an independent review of system activity.
	• On the four NEMIS databases selected for testing, configurations are not fully enabled so that a review of audit trails and activity defined by DHS policy requirements can be completed. Specifically, only failed login attempts are recorded in the audit trails of all database user accounts.
		all NEMIS databases are documented in accordance with DHS and FEMA guidance and the process for audit log review is appropriately implemented for all databases within the NEMIS system boundary.
		• Implement database configurations on all NEMIS databases in accordance with DHS and FEMA policy and procedures over required auditable events and activities.
		• Dedicate the appropriate resources and implement the appropriate automated tools or establish manual processes to collect, review, and retain auditable activities on all NEMIS databases, to ensure compliance with DHS and FEMA policy.			

FEMA-IT-10-10	As noted during the FY 2009 audit engagement, we determined that weaknesses over the tracking of FEMA contractors continue to exist in FY 2010. Specifically: • FEMA does not have a formal process for centrally and adequately tracking FEMA contractors throughout the on-boarding, termination, and transfer processes. As a result, FEMA could not provide a complete	• Develop, document, fully implement, and communicate formal policies and procedures, according to DHS guidelines and requirements, for centrally tracking all contractors throughout the on-boarding, termination, and transfer processes. Ensure policies and procedures include:		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	listing of all contractors working for FEMA. • The process established for notifying FEMA OCIO management, including IT system administrators, of changes in contractor's status, so that accounts can be disabled/removed or account profiles can be appropriately modified in the required timeframe, is not effective or comprehensive. Specifically, no formal requirements exist for COTRs to notify the OCIO of separating contractors.	• The assignment of roles and responsibilities to appropriate FEMA management and stakeholders. • Procedures to ensure that COTRs notify the FEMA OCIO of changes in contractors' status, including separation or transfer, so that accounts can be disabled/removed or account profiles can be appropriately modified in the required timeframe. • Establishment of controls for periodically monitoring the effectiveness of the process to ensure compliance with policy. • Regularly distribute a listing of terminated contractor personnel to information system administrators so they can remove user access timely.			
FEMA-IT-10-11	While FEMA has made improvements over the review of IFMIS-Merger application activity by documenting responsibilities for performing periodic reviews of super user account activities, the following weaknesses noted in FY 2009 continue to exist in FY 2010: • Existing policies and procedures, including FEMA Interim CFO Directive 2600-21, *IFMIS User Access and Termination*, and FEMA SOP 2000-002, *Monitoring of IFMIS Database Audit Log*, do not require the generation, review, or retention of audit logs for all activities required by FEMA and DHS policy. • Failed database (Oracle) and application (UNIX) login	• Revise and implement policies and procedures that document requirements for configuring, retaining, and reviewing audit trails for the IFMIS-Merger application and database, including defined roles and responsibilities, in accordance with DHS and FEMA policy. • Implement configurations on the IFMIS-Merger application and database to ensure that audit logs record required auditable events and activities, in accordance with DHS and FEMA policy. • Implement appropriate management controls to ensure timely communication and implementation of existing and future DHS information security		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	attempts and activity performed by application users with the "super user" role remain the only forms of activity logged and monitored for IFMIS-Merger. Other types of activity required by FEMA and DHS policy, including successful logins, access modifications, and changes to user profiles, are not logged or monitored. • While we noted that logging of users accessing or attempting to access the IFMIS-Merger application is enabled and distributed to appropriate independent reviewers, evidence of review of application login attempts is not documented. Additionally, we noted the following weaknesses related to reviews of activity of super users within the IFMIS-Merger application: • Activity of users with elevated privileges is logged and reviewed on a weekly basis. However, FEMA policy requires that audit records be captured and reviewed at least every three (3) days. • Review of super user activity is performed by an individual with super user privileges within the application, in conflict with segregation of duties principles.	policy requirements pertaining to the configuration of audit logs on the IFMIS-Merger application and database, and to periodically assess system controls to determine compliance.			
FEMA-IT-10-12	The following weaknesses noted in FY 2009 continued to exist in FY 2010: • G&T IFMIS application user accounts were not consistently approved or authorized prior to initial account creation or modification of account privileges. Of the 25 active application users selected for testing,	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010. Any G&T IFMIS accounts which now exist on the IFMIS – Merger instance will need to be included in recertification efforts that will be performed by FEMA as corrective action to remediate NFR FEMA-IT-10-14, which cites a lack of		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	FEMA was unable to provide adequate documented evidence that creation of, or modifications to, account privileges for 22 accounts were properly authorized. Specifically: • Documentation for 10 accounts did not evidence that access was authorized by the OCFO. • Documentation for 11 accounts indicated that access was authorized by the OCFO after the modifications to the account privileges were performed. • Documentation for 1 account was not available. • G&T IFMIS Oracle database user accounts were not consistently approved or authorized prior to initial account creation. Specifically, of the 8 active database user accounts selected for testing, FEMA was unable to provide documented evidence that the initial account creation of 2 accounts in FY 2010 was authorized. While we noted that the planned merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010 and the existing G&T IFMIS Oracle database and application server was decommissioned in June 2010, the weaknesses over the financial data existed for the majority of the fiscal year.	consistent recertification of Core/Merger IFMIS accounts, to ensure that all migrated G&T IFMIS accounts are appropriately authorized.			
FEMA-IT-10-13	As noted during the FY 2009 audit engagement, weaknesses in G&T IFMIS Oracle database audit logging controls continued to exist in FY 2010. Specifically, Oracle database audit trails were not configured to capture any activity, including failed login attempts or	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	administrator-level actions as required by FEMA and DHS guidance. While we noted that the planned merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010 and the existing G&T IFMIS Oracle database was decommissioned in June 2010, the weaknesses over the financial data existed for the majority of the fiscal year.				
FEMA-IT-10-14	During the FY 2010 audit procedures, we noted that weaknesses which existed in FY 2009 related to the recertification of IFMIS application accounts continue to exist. Specifically, although the Core IFMIS application user accounts were recertified in January 2010 prior to the merge of the G&T and Core IFMIS applications, we determined that the recertification of the Core IFMIS accounts was not properly completed. Of the 25 active application accounts selected, FEMA was unable to provide documented evidence that three of the accounts were recertified by the system owner to validate the continued appropriateness of the account, as required by FEMA and DHS policy. Furthermore, these accounts then remained on the IFMIS-Merger application after the merger of the applications occurred.	• Dedicate resources to fully implement FEMA and DHS requirements for a recertification of all IFMIS-Merger application accounts at least annually, including revoking access for any accounts not currently in compliance with the annual recertification. • Identify and implement appropriate monitoring controls to ensure continued compliance with recertification requirements for the IFMIS-Merger application.		X	3
FEMA-IT-10-15	During the FY 2010 audit engagement, we noted that the weaknesses over the recertification of G&T IFMIS application and Oracle database users noted in FY 2009 continued to exist. Specifically, a management review to validate the appropriateness of G&T IFMIS application and Oracle database user accounts was not formally implemented or performed by the OCFO/Financial System Section (OCFO-FSS) this fiscal year.	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010. Any G&T IFMIS accounts which now exist on the IFMIS – Merger instance will be included in recertification efforts that need to be performed by FEMA as corrective action to remediate NFR FEMA-IT-10-14, which cites a lack of consistent recertification of Core/Merger IFMIS accounts.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	We noted that the planned merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010, and the existing G&T IFMIS Oracle database and application server was decommissioned in June 2010. However, prior to the migration of G&T accounts to the IFMIS – Merger instance in February 2010, a recertification of G&T IFMIS application users did not occur. Therefore, the weaknesses over the recertification of users with access to G&T IFMIS financial data existed for the first two quarters of the fiscal year.				
FEMA-IT-10-16	The merger of Core IFMIS and G&T IFMIS was performed in February 2010, and the G&T IFMIS application and database server were formally decommissioned in June 2010. While an ATO was granted for the IFMIS-Merger system by the FEMA CIO on June 4, 2010, prior to the completion of the merged instance, a C&A had not been performed over the G&T IFMIS instance. Consequently, as noted during the prior year FY 2009 audit engagement, G&T IFMIS operated without an ATO prior to its decommissioning. In addition, we determined that during the time the system was operational, neither an ISSO nor a Designated Authorizing Authority (DAA) had been formally designated by FEMA management for G&T IFMIS.	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	2
FEMA-IT-10-17	During the FY 2010 audit engagement, we noted the following weaknesses regarding specialized training for FEMA employees and contractors with significant information security responsibilities: • FEMA has not formally documented or implemented policies and procedures to meet the requirements over specialized training for FEMA employees and	• Develop and implement policies and procedures requiring initial and periodic specialized training for individuals with significant information security responsibilities. • Formally identify specific roles and positions possessing significant information security	X		2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	contractors with significant information security responsibilities in accordance with DHS policy. • With the exception of ISSOs, FEMA has not formally identified all individuals or positions with significant information security responsibilities subject to specialized training requirements. • FEMA does not track or monitor completion of specialized training for FEMA personnel with critical IT roles.	responsibilities that are subject to specialized training requirements. • Develop and implement a mechanism for tracking and monitoring compliance with specialized training requirements for individuals with significant information security responsibilities.			
FEMA-IT-10-18	In FY 2010, we noted that the NEMIS System Security Plan (SSP) was updated in November 2009. However, we determined that the following weaknesses continue to exist: • NEMIS system boundaries, including identification of all hardware and software elements that comprise the NEMIS general support system and subsystems, have not been fully defined. • FEMA has not documented the assignment of FEMA personnel with security responsibilities for the modules and major applications that are classified as NEMIS subsystems within the current NEMIS SSP.	• Fully identify all hardware and software components of the NEMIS platform and update appropriate NEMIS system documentation, including the SSP, to reflect the current operating environment as required by DHS policy and NIST guidance. • Establish and implement a formal process for periodically reviewing and assessing system documentation to ensure that system boundaries and hardware and software components are accurately reflected. • Formally assign and document security responsibilities of FEMA personnel for all components of NEMIS, including all identified modules and major applications.		X	2
FEMA-IT-10-19	During the FY 2010 audit engagement, we noted the following weaknesses regarding configuration management over network devices such as firewalls, routers, and switches that support in-scope financial systems:	• Formally establish roles and responsibilities related to oversight and implementation of configuration management policies and procedures for network devices, including firewalls and routers, supporting financial	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Comprehensive configuration baselines identifying all relevant CIs within the scope of IFMIS and NEMIS have not been documented. • FEMA configuration management policies and procedures require the implementation of Configuration Status Accounting (CSA), which includes recording approved configuration documentation, performing Configuration Audits (CAs), and documenting physical configuration audits to assess conformance with established baselines. However, requirements for the frequency, documentation, and retention of results of these activities have not been defined in existing FEMA policies or procedures. Additionally, the required CSA reports and CAs have not been performed for IFMIS or NEMIS.	applications in accordance with DHS and FEMA requirements. • Revise and implement configuration management policies and procedures over documenting and maintaining current baseline configurations for network devices supporting financial applications, including IFMIS and NEMIS, to ensure DHS and FEMA requirements are adequately addressed and configuration baselines are comprehensively documented by FEMA. Additionally, policies and procedures should include guidance over requirements such as documentation of baselines, periodic review and auditing, and approval of baseline changes for network devices. • Perform required configuration management activities, including periodic CSA and CA activities, for network devices supporting financial applications, including IFMIS and NEMIS, and retain auditable evidence of these activities as required by FEMA policy.			
FEMA-IT-10-20	Conditions noted in FY 2009 related to weaknesses over the documentation and testing of the NEMIS contingency plan continue to exist in FY 2010, as follows: • The NEMIS IT Contingency Plan does not adequately and comprehensively include information required by DHS policy for systems with high impact availability. For example, we noted the following weaknesses: • Detailed information over NEMIS system architecture, such as the database and server	• Update the NEMIS IT Contingency Plan in accordance with DHS and NIST requirements for systems categorized at the high impact availability objective. Additionally, ensure that the Contingency Plan comprehensively addresses the numerous sub-systems within NEMIS so that detailed information exists over the current system architecture, critical processing priorities, detailed recovery procedures and other required components in accordance with DHS guidance.		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	names, as well as information over the various modules of NEMIS, has not been appropriately documented to reflect the current operating environment. • The plan does not sufficiently include details necessary to fully restore NEMIS and dependent subsystems in the event of an emergency. • The contingency plan does not specify critical roles, system resources, or system/application recovery priorities in sufficient detail to distinguish between the various modules within NEMIS. • The Business Impact Analysis (BIA) included in the Contingency Plan was completed in 2004 and is not adequately documented. • Testing of the NEMIS IT contingency plan has not been performed in the past 12 months in accordance with DHS policy.	• Conduct and document annual tests of the NEMIS Contingency Plan that address all critical phases of the plan, and update the Contingency Plan with lessons learned, as necessary and in accordance with DHS and NIST requirements.			
FEMA-IT-10-21	We performed a comparison of active IFMIS-Merger, G&T IFMIS, and NACS accounts, as well as individuals with VPN remote access privileges, against a list of FEMA employees that had separated from employment since October 1, 2009 to determine if any separated employees retained active accounts on the applications or remote access to the FEMA network. The following weaknesses were identified: • 11 IFMIS-Merger user accounts remained active and unlocked after the account holder's separation from FEMA. • 3 G&T IFMIS user accounts remained active and	• Identify the root cause(s) associated with separated employees remaining on FEMA information systems. As appropriate, revise existing procedures or develop additional procedures over removal of separated user access to IT systems to address weaknesses that contribute to untimely removal of separated individuals from the systems. • Ensure that procedures are implemented consistently to remove system and application accounts for all separated users immediately upon notification of separation, in accordance with		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	unlocked after the account holder's separation from FEMA. • 164 NACS accounts with NEMIS positions assigned at the time of our test work remained active and unlocked after the account holder's separation from FEMA. • 33 individuals retained the ability to access the FEMA network remotely due to active VPN remote access privileges after the account holder's separation from FEMA. All 33 individuals additionally retained an active NACS account as described above, thus allowing them to potentially access NEMIS as well.	FEMA, DHS and NIST guidance. No corrective action specific to the portion of this finding related to G&T IFMIS will be provided because of the decommissioning of that system in June 2010.			

FEMA-IT-10-22	In FY 2010, we noted that the following conditions identified in FY 2009 related to FEMA LAN accounts continue to exist:
	• The FEMA LAN domain security policy does not enforce password requirements in accordance with DHS policy. Specifically:
	  • The FEMA LAN does not enforce a password history or prevent reuse of passwords.
	  • The FEMA LAN does not enforce complexity requirements, including password length or the use of mixed-case alphanumeric and special characters, to ensure that strong passwords are used.
	• FEMA was unable to provide evidence of account authorization for 10 Active Directory (AD) individual user accounts created in FY 2010.
		• Configure the FEMA LAN to ensure compliance with DHS and FEMA policy requirements for passwords and authenticator control requirements, including expiration, reuse, length, and complexity.
		
		• Identify and implement appropriate monitoring controls to ensure that all accounts on the FEMA LAN are in compliance with DHS requirements for authorization. Additionally, ensure that where appropriate policies and procedures are further developed and/or revised to ensure consistent implementation and include requirements for all accounts on the FEMA LAN, including generic, shared group, service, and LAN end-user accounts not included in the NACS.
		
		• Develop and implement a formal process for performing a periodic recertification of all FEMA
				X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	• While policies and procedures over the authorization of generic, shared group, and service accounts on the FEMA LAN have been finalized, approval of these accounts is not consistently documented according to policy. Specifically, of a selection of 45 generic, group, and service LAN accounts created during FY 2010:
	  • 2 did not have a clearly defined business need or justification documented;
	  • 26 did not have IT Security or system owner approval documented;
	  • 19 were created prior to supervisory certification; and
	  • 2 did not have any authorizing documentation provided for our review.
	• FEMA has not established procedures and implemented a process over the periodic recertification of FEMA LAN accounts to ensure that access is still necessary and appropriate for each account as required by FEMA and DHS policy.
	• We compared a listing of active FEMA LAN/AD accounts against a list of FEMA employee separations that had occurred since October 1, 2009 and determined that 85 accounts remained active and unlocked after the account holder's separation from FEMA.
		LAN accounts which defines requirements and addresses accounts not included during the planned recertification of NEMIS application access.
		• Evaluate and, if appropriate, revise existing procedures over removal of separated user access to the FEMA LAN to ensure the timely removal of separated individuals from the network.
		• Ensure that procedures are implemented consistently to remove FEMA LAN accounts for all separated users immediately upon notification of separation, in accordance with FEMA, DHS and NIST guidance.			

FEMA-IT-10-23	In FY 2010, we determined that while change management procedures have been developed and	We recommend that FEMA OCIO and NFIP management finalize and implement comprehensive		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	implemented for applications hosted by the NFIP LAN, including Traverse, the documented procedures do not specifically address patch management policies and procedures for the NFIP LAN in accordance with DHS requirements. Specifically, controls over the approval, testing, and deployment of operating system patches are not addressed.	patch management policies and procedures for the NFIP LAN supporting Traverse, in accordance with DHS policy. Additionally, FEMA and NFIP management should ensure that these procedures include requirements for authorizing, testing, and approving patches to be implemented into production and responding to DHS Security Operations Center and DHS Enterprise Operations Center (EOC) notifications to ensure compliance with the timely implementation of required patches.			
FEMA-IT-10-24	During FY 2010, we noted that weaknesses over the C&A of NFIP continue to exist. Specifically, • FEMA approved *Conditional ATOs* for the NFIP/Legacy System Services (LSS) on May 22, 2009 and August 20, 2010 for two one-year periods. However, we noted that in the absence of a full ATO, DHS policy allows "interim" ATOs only for systems that are either under development testing or in the prototype phase of development, not operational systems such as the NFIP/LSS. Additionally, "interim" ATOs cannot exceed two consecutive six-month periods. • During the initial *Conditional ATO* period that began on May 22, 2009, FEMA did not complete C&A efforts, including the risk assessment and Security Testing and Evaluation (ST&E) needed to fully assess risk associated with the system, so that a full ATO could be issued. Consequently, from May 2010, when the initial *Conditional ATO* expired, through August 2010 when the second *Conditional ATO* was approved, the system operated without any	We recommend that NFIP continue to work with the FEMA OCIO to complete the recertification and accreditation of the NFIP Legacy Services System, including documentation of all required artifacts in accordance with applicable DHS policies and Federal guidance.		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	authorization. • During our audit fieldwork period, NFIP was unable to provide us with evidence that C&A activities required to be performed for a full ATO to be granted had been completed.				
FEMA-IT-10-25	During the FY 2010 audit engagement, we noted that the following conditions related to management of FEMA VPN accounts continue to exist: • The *VPN Rules of Behavior for Users Behind Corporate Firewalls*, dated December 5, 2002, requires individual's manager approval and Enterprise Service Desk (ESD) validation of all VPN Access Request forms prior to granting access. However, approval by the system owner or a designated representative is not required. • *VPN Access Request* forms include an approval block titled "For FEMA OCS Use Only," and the form states that all VPN requests must be approved by the FEMA Office of Cyber Security (OCS). However, OCS does not currently exist as a FEMA Division due to FEMA's reorganization. Consequently, existing policies and procedures do not reflect the current security management structure at FEMA nor do they assign responsibility to a current entity within the agency. • A periodic recertification of FEMA VPN access accounts is not currently performed to ensure that remote access is still necessary and appropriate for each individual.	• Revise and implement current policies and procedures for documenting, reviewing, and approving all remote access accounts to the FEMA LAN including VPN and iPass access. Specifically, roles and responsibilities should be defined to ensure that sufficient resources are dedicated to appropriately authorize accounts on behalf of the system owner or a designee prior to granting remote access, according to FEMA and DHS policy. • Develop and implement policies and procedures to perform a periodic recertification of all remote user access and retain auditable records as evidence that recertifications are conducted and completed in accordance with DHS and FEMA policy.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	• Of the selection of 45 *VPN Access Request* forms reviewed:
	  • Two did not specify the date that access was approved by the requestor's supervisor.
	  • Three were granted supervisory approval after VPN access was established for the user.
	  • The section of each form that required "OCS" level review and approval was not completed.
	Additionally, we conducted further testwork over remote access granted through the iPass utility, which is used to provide dial-up access to the FEMA network via the VPN gateway. This access is managed through a separate access authorization process from VPN. During our testwork, we noted the following new conditions in FY 2010 related to management of access to iPass:
	• While *iPass User Agreement* forms require Section Chief (or equivalent) approval and IT certification for iPass remote access, requests are not approved by the system owner or a designated representative, as required by DHS policy. Additionally, policies and procedures do not exist related to the granting and management of users of the iPass remote dial-up utility.
	• Of the selection of 45 *iPass User Agreement* forms reviewed:
	  • Three did not specify the date that access was approved by the requestor's section chief (or equivalent).				

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• One was granted supervisory approval after VPN access was established for the user. • One was granted supervisory approval by the same individual that the requested VPN account was for, indicating a violation of segregation of duties in the management review and approval of information system access.				
FEMA-IT-10-26	The following weaknesses noted in FY 2009 continue to exist in FY 2010: • IFMIS-Merger application user accounts were not properly approved or authorized. Specifically, of the 25 active application users selected for review, FEMA was unable to provide documented evidence that initial account creation or the most recent modifications to account privileges for 6 accounts were authorized. • Policies and procedures over the management of accounts on the IFMIS-Merger Oracle database do not specify requirements for performing a periodic recertification of database accounts to validate the continued appropriateness of access. • IFMIS-Merger Oracle database user accounts were not properly approved or authorized. Specifically, of the eight active database users selected for review, approval for six user accounts was not documented prior to creation of the accounts. Approval was not documented for these accounts until after the audit request for documentation was received. • The FY 2010 recertification of IFMIS-Merger Oracle	• Identify and implement appropriate monitoring controls to ensure compliance with initial authorization and modification requirements for accounts on the IFMIS-Merger application. • Document policies and procedures over the periodic recertification of all accounts on the IFMIS-Merger database. • Dedicate resources to fully implement FEMA and DHS requirements for a recertification of all IFMIS-Merger database accounts at least annually, including revoking access for any accounts not currently in compliance with the annual recertification. • Identify and implement appropriate monitoring controls to ensure compliance with initial authorization, modification, and periodic recertification requirements for accounts on the IFMIS-Merger database.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	database user accounts was neither completed consistently nor in accordance with FEMA policy. Specifically, we requested a selection of recertification forms for eight IFMIS-Merger database user accounts and determined that three were granted to contractors, but COTR approval was not documented.				

FEMA-IT-10-27	As noted during the FY 2009 audit engagement, the following weaknesses in G&T IFMIS Oracle database user account password controls continued to exist in FY 2010:
	• We determined that FEMA performed manual reviews of inactive G&T IFMIS database accounts on a monthly basis to disable accounts which had not been used in the prior 90 days. However, since G&T IFMIS is categorized as a high impact system, reviews are required to disable accounts that have been inactive for 45 days, according to DHS policy.
	• The G&T IFMIS database account security policy did not enforce password requirements in accordance with DHS policy. Specifically:
	  • The database did not enforce a password history or prevent reuse of passwords.
	  • The database did not enforce complexity requirements, including definition of a password verification function to ensure strong passwords are used. Specifically, password length and requirements over the use of mixed-case, alphanumeric and special characters to enforce restrictions over the use of dictionary words, are not defined.
		There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• The database did not enforce password expiration after a predetermined length of time. • FEMA had not established a formal process for approving emergency and temporary access to the G&T IFMIS database that is compliant with DHS requirements. Specifically, emergency and temporary access to the database for individuals with elevated privileges, including access for contractor development personnel, is approved by the FSS Chief and/or his/her staff, not by the FEMA Chief Information Security Officer (CISO) or a designee, as required by DHS policy. Additionally, a formal process specifically addressing procedures for the granting of temporary access to the database and ensuring that access is removed in a timely manner was not documented within existing IFMIS access control policies and procedures. Furthermore, we determined that through this process the G&T IFMIS Oracle database access was granted to contracted development personnel in order to implement database changes to G&T IFMIS, which continues to conflict with segregation of duties principles. While we noted that the merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010 and the existing G&T IFMIS Oracle database was decommissioned in June 2010, the weaknesses noted existed for the majority of the fiscal year.				
FEMA-IT-10-28	Weaknesses noted in FY 2009 over C&A of the FEMA LAN and subsystems that host in-scope financial applications continue to exist in FY 2010. During our FY 2010 audit engagement, we noted that FEMA has	• Continue to fully identify and decouple all components of the FSN-2 platform, including regional LANs and GSSs, which host or support IFMIS and NEMIS, and perform all required		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	classified regional LANs as subsystems and included them within the defined system boundary of the FEMA Switched Network (FSN)-2. We noted the following weaknesses in the C&A of the FSN-2 General Support System (GSS) that includes the FEMA LANs:
	• The FSN-2 GSS C&A was not completed in compliance with DHS and NIST requirements and has not been updated to accurately reflect the current GSS environment. Specifically:
	  • The authorizing officials and individuals noted as responsible for the security roles for multiple regional LANs and subsystems are not accurately reflected in the SSP included in the C&A package as employees with specified roles no longer work for FEMA in the capacity noted.
	  • While the Maryland National Processing Service Center is identified as a subsystem in the overarching FSN-2 GSS C&A package SSP, C&A activities have not been performed over this subsystem.
	  • DHS policy requires annual testing of IT contingency plans for information systems with a high impact availability categorization, such as the FSN-2 GSS. However, the most recent test of the FSN-2 IT contingency plan was performed and documented during FY 2008.
	  • DHS policy requires that risk assessments be conducted for information systems no less frequently than every three years. However, the most recent ST&E was documented during FY
		C&A activities over each component as required by DHS policy and NIST guidance.
		• Formally assign and document security responsibilities for all components of the FSN-2 platform, including regional LANs and GSSs, which host or support IFMIS and NEMIS.			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	2006. • The most recent ATO granted by the FEMA CIO expired on January 22, 2010, and the FSN-2 GSS is currently operating without authorization from FEMA management. • Although the 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 the production servers for NEMIS and IFMIS applications. Consequently, we were unable to test the hosting environment supporting financial applications in-scope for the FY 2010 environment.				
FEMA-IT-10-29	During the FY 2009 audit engagement, we noted that a C&A of PARS had not been performed and the system had not received an ATO since becoming operational in the FEMA environment. While improvements were noted in this condition for FY 2010, we determined that the following C&A weaknesses over PARS continue to exist: • In FY 2010, the PARS database was included within the accreditation boundary for the IFMIS-Merger system, which was granted an ATO in June 2010. However, prior to that date, the PARS database was not certified and accredited and consequently, operated without an ATO for the majority of FY 2010. • All other system components of PARS, including the web and application servers, continued to operate	• Formally designate an ISSO for the PARS web server and application environment. • Certify and accredit the PARS web server and application environment, including documentation of all required artifacts in accordance with applicable DHS policies and Federal guidance.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	without an ATO, and evidence that C&A efforts for these components of PARS were completed and approved by FEMA management could not be obtained from FEMA for review during the FY 2010 audit engagement. • At the time of our test procedures, an ISSO had not been formally designated by FEMA management for the PARS web server and application. While we were informed by FEMA IT Security Management that the PARS database was administered by an ISSO under the Core IFMIS, we determined that no formal designation of this responsibility was assigned until FY 2010 because the PARS database was not included in the C&A boundary for Core IFMIS and no additional designation letters were issued. As a result, the PARS database did not have a formal designation of security responsibilities for the majority of the fiscal year.				
FEMA-IT-10-30	As noted during the FY 2009 audit engagement related to Core IFMIS, we determined that weaknesses over the authorization of emergency and temporary access to the IFMIS – Merger Oracle database continue to exist in FY 2010. Specifically, FEMA has not established a formal process for approving emergency and temporary access to the IFMIS-Merger database that is compliant with DHS requirements. During our FY 2010 testing, we determined that emergency and temporary access to the database for individuals with elevated privileges, including access for contractor development personnel, is approved by the FSS Chief and/or his/her staff, not by the FEMA CISO or a designee, as required by DHS policy. Additionally, a formal process specifically addressing procedures for the	Document and implement a formal process for granting emergency and temporary access to the IFMIS-Merger database that includes guidance over all types of accounts authorized for temporary and emergency access, segregation of duties considerations, and appropriate approval from FEMA management in accordance with DHS policy.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	granting of temporary access to the database and ensuring that access is removed in a timely manner has not been documented within existing IFMIS-Merger access control policies and procedures. Furthermore, we determined that through this process the IFMIS-Merger Oracle database access is granted to contracted development personnel in order to implement database changes to IFMIS-Merger, which continues to conflict with segregation of duties principles.				
FEMA-IT-10-31	During our unannounced enhanced security testing performed during the FY 2010 audit engagement, we noted that the FEMA Security Operations Center (SOC) proactively tracked and reported incidents related to social engineering attempts performed at FEMA headquarters and regional offices through implemented ad hoc processes. However, weaknesses noted during the FY 2009 audit engagement related to FEMA's incident response program continue to exist in FY 2010. Specifically, standard operating procedures for the management of FEMA IT security incidents have not been formally approved and implemented by FEMA management. Consequently, FEMA has not implemented DHS policy requirements to establish a documented and formally approved component-level incident response framework or capability, including roles, responsibilities, and processes related to the identification, evaluation, and resolution of all security incidents.	Formally approve and implement procedures for managing security incidents. Specifically, procedures should clearly outline roles and responsibilities required to maintain a continuous incident response capability and define processes related to the identification, evaluation, and resolution of all security incidents, as required by DHS and FEMA policy.		X	3
FEMA-IT-10-32	In FY 2009, we identified weaknesses over FEMA's patch management program as it relates to Core IFMIS and G&T IFMIS. During the FY 2010 audit engagement, we	Further dedicate resources to document and fully implement comprehensive system-specific patch management procedures to ensure that IFMIS-Merger		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	determined that while FEMA has finalized and formally implemented the *FEMA Office of the Chief Information Officer (OCIO) Standard Operating Procedure (SOP) for Vulnerability Patch Management*, the SOP was not approved until April 8, 2010. Consequently, FEMA did not have a formal patch management procedure applicable to the IFMIS environments for a majority of the fiscal year. Given the timing of the SOP's approval, the patch management procedures could not be implemented when G&T IFMIS was operational as it was merged with Core IFMIS in February 2010. Additionally, we determined that FEMA has not fully and consistently implemented the requirements and procedures documented in the SOP for IFMIS-Merger in accordance with FEMA and DHS guidance.	operating system and database patches are tested and deployed in a timely manner, in accordance with DHS and FEMA policy. No corrective action specific to the portion of this finding related to G&T IFMIS will be provided because of the decommissioning of that system in June 2010.			
FEMA-IT-10-33	Weaknesses noted in FY 2009 over FEMA's information security vulnerability management program as it relates to NEMIS continue to exist in FY 2010. Specifically: • FEMA does not have documented and approved procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of NEMIS. • The list of NEMIS servers currently scanned by the SOC is incomplete and does not represent the current NEMIS system boundary as defined by system owners and IT security management. Additionally, NEMIS system owners are not receiving listings of all vulnerabilities noted on their system components to ensure corrective action is tracked and remediated. • Corrective action over vulnerabilities identified	• Establish and implement documented procedures that define formal requirements, processes, and responsibilities for performing periodic vulnerability scans of NEMIS production servers. Additionally, ensure these procedures include requirements for reporting and tracking resolution of weaknesses identified during internal NEMIS vulnerability scans in accordance with DHS POA&M guidance. • Revise listing of NEMIS servers scanned by the FEMA SOC to ensure that vulnerability scans performed include all NEMIS servers within the current operating environment. Additionally, develop and implement procedures to ensure that this listing is periodically re-evaluated and		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	through SOC internal scans of NEMIS production servers is not formally tracked via the POA&M process, as required by DHS policy.	updated as appropriate. • Revise the SOC distribution listing of NEMIS system owners and other appropriate IT security management to further define personnel responsible for remediating and formally tracking all vulnerabilities identified over the various NEMIS components. Additionally, develop and implement procedures to ensure that this listing is periodically re-evaluated and updated as appropriate.			
FEMA-IT-10-34	Weaknesses noted in FY 2009 over FEMA's information security vulnerability management program as it relates to G&T IFMIS and IFMIS-Merger continue to exist in FY 2010. Specifically: • FEMA did not have documented and approved procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of G&T IFMIS and IFMIS-Merger. • For one of the three months selected for testing, vulnerability scans were not performed for the G&T IFMIS production server. • For all three months selected for testing, vulnerabilities reported by the FEMA SOC over the G&T IFMIS and IFMIS-Merger production servers were not formally tracked via the POA&M process, as required by DHS policy.	Establish and implement documented procedures that define formal requirements, processes, and responsibilities for performing regular vulnerability scans of IFMIS-Merger. Additionally, procedures should include requirements for reporting and tracking resolution of weaknesses identified during internal IFMIS-Merger vulnerability scans in accordance with DHS POA&M guidance. No corrective action specific to the portion of this finding related to G&T IFMIS will be provided because of the decommissioning of that system in June 2010.		X	3
FEMA-IT-10-35	In FY 2009, we identified weaknesses over FEMA's patch management program related to NEMIS. During the FY	Further document and fully implement comprehensive system-specific patch management procedures to		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	2010 audit engagement, we determined that while FEMA has finalized and formally implemented the FEMA OCIO SOP for Vulnerability Patch Management, the SOP was not approved until April 8, 2010. Consequently, FEMA did not have a formal patch management procedure applicable to the NEMIS environment for a majority of the fiscal year. Additionally, we determined that FEMA has not fully and consistently implemented the requirements and procedures documented in the SOP for all NEMIS components in accordance with FEMA and DHS guidance.	ensure that NEMIS operating system and database patches are tested and deployed in a timely manner, in accordance with DHS and FEMA policy. Additionally, these policies and procedures should include formal designation of responsibilities for oversight and implementation of required patch management activities for all NEMIS components to ensure compliance at the system level.			
FEMA-IT-10-36	Weaknesses identified in FY 2009 related to the testing of NEMIS production database backup tapes continue to exist in FY 2010. Specifically: • During two quarters of FY 2010, FEMA conducted restoration tests of backup tapes for one specific NEMIS database while FEMA's SOP for Tape Backup Testing documents requirements for the testing of 39 databases. Consequently, we determined that FEMA did not regularly test backup tapes containing all NEMIS production database data during the fiscal year. • Additionally, while we noted that the SOP for Tape Backup Testing assigns responsibility for testing backup tapes in accordance with a defined schedule to NEMIS IT security management, administrators, and system owners, the SOP was not updated to reflect the required schedule for performing tape restoration tests. Furthermore, we noted the following new weaknesses related to controls over the performance of NEMIS	• Develop and implement backup policies and procedures to ensure that all NEMIS components are backed up and backup media is stored in/rotated to an off-site facility according to FEMA and DHS requirements. • Revise or develop policies and procedures to periodically test and document testing of the NEMIS backups in compliance with FEMA and DHS requirements. In addition, ensure that policies and procedures are implemented to perform periodic restoration testing of all NEMIS production databases in accordance with established requirements.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	database backups: • FEMA has not formally defined and documented procedures that outline processes for performing backups of NEMIS production databases and for rotating and physically securing backup tapes off-site. • FEMA was unable to provide requested documentation to evidence that any of the 39 NEMIS production databases identified in the SOP for Tape Backup Testing are currently being backed up.				
FEMA-IT-10-37	During our social engineering testing, several personnel provided us with user IDs and/or passwords. It should be noted that several personnel that we contacted by phone during our social engineering phone calls challenged our requests for user access credentials by looking up our assumed names in the FEMA directory to determine if we were FEMA personnel, requesting employee IDs, asking for help desk ticket numbers associated with our calls, and reporting our attempts to supervisors. While individuals contacted represented several offices in multiple FEMA regions as well as Headquarters, our selection of individuals was not statistically derived. Therefore, we are unable to project these results to FEMA as a whole.	Review the effectiveness of existing security awareness programs designed to protect "need-to-know" information, including IT system access credentials, 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.	X		3
FEMA-IT-10-38	During our after-hours physical security testing conducted on July 20, 2010, we noted instances of improperly protected authentication credentials, system information, information technology assets, and Personally Identifiable	Review the effectiveness of existing security awareness programs designed to protect electronic and physical data, PII, and For Official Use Only (FOUO) agency information and ensure that individuals are adequately instructed and reminded of		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Information (PII) in the facilities inspected. Some of the instances of improperly secured PII noted consisted of large stacks of documents or compiled spreadsheets that contained PII for numerous individuals conducting business for or with FEMA. Exceptions categorized as "Other' consisted of laptops and other IT assets not physically secured/locked to workspaces, unsecured bank account and government travel card information, and the lack of adequate locking mechanisms on a server room door. Our selection of areas at each facility that were inspected was not statistically derived, and therefore, we are unable to project results to FEMA as a whole.	their roles in the protection of both electronic and physical FEMA data and hardware through formal, periodic communications and/or security awareness training.			
FEMA-IT-10-39	As noted during the FY 2009 audit engagement, weaknesses continue to exist over the segregation of duties controls for the migration of IFMIS-Merger changes into production. Specifically: • The FEMA development contractor continues to deploy changes into the UNIX production environment through the use of the shared "ifmiscm" account. We noted that FEMA change management personnel are following SOPs that outline the controls intended to mitigate the risk associated with the IFMIS-Merger developers having the ability to migrate changes to the IFMIS-Merger production environment. In particular, the *Office of the Chief Financial Officer (OCFO) IFMIS System Change Request (SCR) SOP* requires the locking and unlocking of the "ifmiscm" account by system administrators during the implementation of software changes into production. However, we determined	Document and implement policies and procedures to limit IFMIS-Merger developer access to the production environment to "read only" and segregate the responsibility for deploying application code changes into production from the development contractor to an independent control group. If business needs require that the segregation of duties cannot be immediately implemented, document and implement policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance, including a formalized process for performing and documenting reviews of activity performed by developers within the IFMIS-Merger environment.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	that while the SCR SOP states that system administrators will periodically monitor production directories to detect updates, no formal procedures or processes are included in the SOP or documented elsewhere for detailing how to monitor the directories or the requirements for performing the reviews to verify that only authorized changes to the "ifmiscm" directory and sub-directories are implemented into production by the developers. • We determined that although informal reviews of the directories were performed during the fiscal year, they were not routinely relied upon by FEMA management as they did not provide the level of detail required for adequate monitoring, and FEMA personnel were not able to distinguish the types of changes made to the system from the "ifmiscm" account.				
FEMA-IT-10-40	As noted during the FY 2009 audit engagement, weaknesses continued to exist over the segregation of duties controls for the migration of G&T IFMIS changes into production during FY 2010. Specifically, the "ifmiscm" account was used by the FEMA development contractor to deploy changes into the UNIX production environment. Per our review, we noted that the G&T IFMIS application programmers responsible for maintaining and developing changes for the G&T IFMIS application were also responsible for migrating application code changes into the production environment using the "ifmiscm" account. We were informed by FEMA personnel that the controls over this account did not change from FY 2009 and that the account remained unlocked while G&T IFMIS was operational between	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	October 2009 and June 2010 when the system was decommissioned. We were further informed by FEMA personnel that access to the "ifmiscm" account was not limited or monitored on a periodic basis, allowing the development contractor unrestricted access to the production environment. Additionally, we noted that FEMA has documented policies and procedures that require the IFMIS-Merger "ifmiscm" account to be locked and use of the account to be monitored. However, we noted that no established procedures or controls were in place for G&T IFMIS to mitigate the risk associated with this account. Consequently, we determined that while the G&T IFMIS application server was decommissioned in June 2010, the weaknesses over segregation of duties controls in the G&T IFMIS configuration management process continued to exist for the majority of FY 2010, and prior year NFR FEMA-IT-09-59 is reissued.				
FEMA-IT-10-41	Password, patch management, and configuration management weaknesses were identified during vulnerability assessment technical testing. *Note: Due to the nature of this finding, see the tables in associated NFR for the specific details of the conditions.*	Implement the specific corrective actions listed in the NFR for each technical control weakness identified.		X	3
FEMA-IT-10-42	During the FY 2010 audit engagement, we noted the following weaknesses over the completeness and accuracy of certain C&A artifacts that support the Authorizing Official's decision to grant an ATO for the IFMIS – Merger: • A risk assessment for IFMIS-Merger had not been	• Update and complete all required C&A artifacts for IFMIS-Merger in accordance with DHS policy and NIST guidance. • Ensure that C&A artifacts, including the risk assessment or the results of the required risk assessment activities, the ST&E, and the Security	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	completed or documented prior to granting an ATO, in accordance with DHS and NIST requirements. Additionally, FEMA does not plan to conduct and document a risk assessment or the results of the required risk assessment activities for IFMIS-Merger as FEMA management has indicated that it is not required for FY 2010. • The ATO was signed in June 2010, more than three months after the IFMIS-Merger system was operational in late February 2010. • Per our review of the security assessment report, the assessment performed over IFMIS-Merger prior to granting ATO did not include evaluation of any of the controls identified within the SSP. The assessment was limited to vulnerability and compliance scans. • The ST&E was not properly conducted because the baseline controls in the Requirements Traceability Matrix were not consistent with DHS requirements.	Assessment Report (SAR) are conducted and documented in accordance with established DHS baseline controls according to the security categorization of the system.			
FEMA-IT-10-43	During the FY 2010 audit engagement, we noted that the most recent ATO for NEMIS was signed on October 29, 2009. However, we identified weaknesses in the completeness and accuracy of certain C&A artifacts that support the Authorizing Official's decision to grant the ATO for NEMIS. Specifically, the NEMIS Risk Assessment, ST&E, and SAR were completed in 2006, and thus outdated as DHS policy requires C&A artifacts supporting ATOs to be updated within the 13 months prior to granting the most recent ATO, and NIST requires each to be conducted every 3 years.	Update and complete all required C&A artifacts for NEMIS in accordance with DHS policy and NIST guidance.	X		3
FEMA-IT-	Conditions noted in FY 2009 related to weaknesses over	Document and implement appropriate technical and		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
10-44	controls in place to monitor and restrict access to highly-privileged system accounts within the UNIX environment that supports IFMIS-Merger and G&T IFMIS continue to exist in FY 2010. Specifically: • Access to the "root" account is not properly restricted and system administrator activities are not appropriately logged. Specifically, the password to access the UNIX "root" administrator account is shared between the administrators, and remote access to the root account is not locked down. • System administrator actions are not monitored and attributable to individual administrators. Specifically, FEMA has not enforced the use of the "sudo" command, which requires system administrators to login with their individual user ID and then switch over to the root account to ensure who is accessing the account is logged and authorized. • System logs and reports of administrator activity, including the "sudo" log which monitors actions performed by administrators while acting as the "root" account, were not reviewed by FEMA management personnel independent of the system administration staff.	management controls to restrict and monitor access to privileged system administrator accounts on the IFMIS-Merger operating system, including use of the "root" account, in accordance with DHS and FEMA policy. Additionally, policies and procedures should include requirements to ensure that system logs and records of administrator activity, including the "root" account, are retained and reviewed by IT security management independent of the system administration team, especially where individual traceability for the account is not possible. There is no recommended corrective action specific to the portion of this finding related to G&T IFMIS because of the decommissioning of G&T IFMIS in June 2010.			
FEMA-IT-10-45	In FY 2009, we noted weaknesses over suitability determinations for federal employees and contractors with sensitive IT system access that continued to exist in FY 2010. Specifically, of 15 federal employee positions selected for testing: • Three did not have evidence of a completed background investigation on file that met minimum	• Further define and refine documented processes to ensure that background investigations for all Federal employees are performed and procedures are implemented in accordance with DHS directives. • Reevaluate and assign the correct position sensitivity levels to all Federal employees with		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	investigative requirements specified by DHS policy. • For one employee, FEMA was unable to provide any documentation to evidence that the employee's background investigation was performed and maintained within the Integrated Security Management System (ISMS), FEMA's personnel suitability and investigation recordkeeping utility. • Nine that are defined as "high risk" according to FEMA policy did not have an appropriate position sensitivity designation that reflected the risk level required by DHS policy. During our FY 2010 test work over contractors, we determined that no formal procedures have been developed or implemented by FEMA to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. Additionally, we selected a population of 15 contractors with access to multiple FEMA information systems who hold sensitive IT security positions at FEMA such as system administrators, database administrators, and systems development contractors and determined that FEMA has not appropriately conducted suitability investigations. Specifically: • For two, FEMA was unable to provide any documentation to evidence that the contractor's record was maintained within ISMS, including the status of any background investigations performed. • Six did not have evidence of a completed background investigation on file that meets	access to DHS information systems in accordance with DHS policy. Additionally document and/or revise, and fully implement procedures to ensure that program managers are aware of requirements and appropriate position sensitivity levels are designated for all sensitive IT positions in the future. • Document and fully implement procedures within FEMA Acquisitions, FEMA Personnel Security, and FEMA IT to ensure a more centralized and coordinated process for tracking and completing background investigations over contractor personnel in accordance with DHS policy. • Ensure that all system owners document and correctly define the appropriate sensitivity designations for contractor personnel needing access to their information systems in accordance with DHS policy. Additionally, ensure that position sensitivity designations are assigned based on the type of privileges needed, and require contractors to have their suitability investigations completed prior to being granted access to the system in accordance with FEMA and DHS policy.			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	minimum investigative requirements specified by DHS policy. Of the six, two had records maintained within ISMS; however, FEMA was unable to provide evidence that background investigations for each were performed. • None had position sensitivity designations defined by FEMA for the sensitive IT position they held at the time of our test work, as required by DHS policy.				
FEMA-IT-10-46	During the FY 2010 audit engagement, we noted weaknesses in controls over the configuration management of application, web, and database servers within the NEMIS production environment. Specifically: • Access to the multiple application, web, and database servers that comprise the NEMIS production environment for deploying approved code changes is limited to IT Enterprise Operations staff. However, no formalized change management procedures exist for deploying changes to ensure the movement of production code for the NEMIS production environment is appropriately controlled. • Access to a shared service account is used for the deployment of Linux[5] changes. However, FEMA was unable to provide any system documentation or associated artifacts demonstrating that FEMA was appropriately restricting and controlling access to the	• Document and implement a formalized process and procedures for deploying NEMIS changes to ensure the movement of production code for the NEMIS production environment is appropriately controlled. Procedures should include requirements for restricting and, monitoring access and documenting reviews to the NEMIS production environment to ensure that the principles of least privilege and segregation of duties are enforced, in accordance with DHS guidance. • Ensure that adequate technical controls are implemented to enforce least privilege and segregation of duties requirements for the implementation of system changes. If individual accounts are not possible for deploying changes, implement logical access controls, including configuration of system audit logs, on NEMIS production servers to establish individual		X	3

[5] Linux is one of the operating system platforms that the NEMIS application resides on and houses the production source code directories for a portion of the NEMIS modules.

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	NEMIS production application, web, and database servers.	accountability for all FEMA personnel with access to the environment through the shared service account, in accordance with DHS and FEMA policy. Additionally, for these shared service accounts, document, implement, and approve standard operating procedures for the implementation and formal review of NEMIS system changes on production servers.			
FEMA-IT-10-47	In FY 2009, we noted that FEMA's OCFO and NFIP financial systems development and acquisition projects were undertaken and progressed without (1) proper oversight of and direction to contractors, (2) development and approval of required project documentation, (3) the continual involvement of the OCIO to ensure appropriate consideration and integration of IT security, and (4) the joint communication and decision-making of FEMA OCFO, OCIO and NFIP management. As a result, we recommended that FEMA management define and implement formal and repeatable processes to ensure that financial systems development and acquisition projects are conducted in compliance with DHS SELC and acquisition requirements as well as Federal guidance. During the FY 2010 audit engagement, we determined that FEMA management has not implemented corrective actions or developed a corrective action plan to address the prior year weaknesses noted. Specifically, entity-level corrective actions to integrate and develop sufficient and effective methods of communication to ensure that significant financial-related system development and acquisition projects involve all relevant stakeholders,	• Define and implement formal and repeatable entity level control processes to ensure that financial systems development and acquisition projects are conducted in compliance with DHS SELC and acquisition requirements as well as Federal guidance. The processes should define steps to include, but are not limited to, formal approval of required project documentation, sufficient contractor oversight, definitions of project roles and responsibilities so that decision making includes the appropriate involvement of all stakeholders and relevant FEMA management, establishment of Acquisition Decision Events (ADEs) at each SELC phase, and integration of IT security considerations throughout all project phases. • Identify and formally assign stakeholders associated with the remediation efforts over aligning the DHS SELC methodology with FEMA's acquisition development process to ensure appropriate participation from all required organizations within FEMA in both the development of policies and procedures and integration of the financial systems acquisitions		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	including the OCFO, have not been established. Additionally, FEMA management has not taken action to enhance and further develop current acquisition management processes to ensure that organization-specific requirements exist and are implemented so that each project meets organizational mission needs and functional and technical requirements as required by DHS and NIST guidance.	life cycle stages as required by DHS policy.			
FEMA-IT-10-48	FEMA IT security management responsibilities were not consistently or adequately assigned and performed over the FEMA POA&M process for FY 2009 IT audit findings, in accordance with DHS guidance. Specifically: • POA&Ms created by FEMA management in response to FY 2009 IT financial statement audit findings were not consistently categorized with the appropriate criticality level in accordance with DHS policy. Specifically, for 52 POA&Ms provided by FEMA on May 3, 2010, criticality was either undefined or erroneously defined as "Annual Assessment Finding" rather than "Initial Audit Finding" or "Repeat Audit Finding," as required. • FEMA management did not consistently document detailed corrective action plans or appropriate milestones, including required tests of design and effective implementation for financial system POA&Ms. • FEMA management did not consistently assign POA&M stakeholder ownership for corrective action plans or related milestones.	• 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. • Dedicate resources to fully implement DHS requirements over the POA&Ms for audit findings of FEMA financial systems, including the proper categorization of audit findings, documentation of all stakeholders with remediation responsibilities, and monitoring of POA&M activities to validate that corrective actions are appropriately documented with associated milestones and evidence of remediation is developed and retained. • Develop and implement a training program for personnel with IT security responsibilities, such as system owners and ISSOs, to ensure that they fully understand their roles and responsibilities to correctly categorize the findings, formally define milestones, and validate the documentation and	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		testing of the corrective action implemented. • Develop and implement review procedures to ensure developed POA&Ms are detailed enough to demonstrate that the root cause of the issue has been assessed and the milestones address the necessary steps to fully remediate the weaknesses as required by DHS policy.			
FEMA-IT-10-49	During the FY 2010 follow-up testwork, we determined that weaknesses noted in FY 2009 continue to exist. Specifically, we determined that no additional policies and procedures to establish a process for implementing change controls for the maintenance of system security functions have been developed by FEMA or the IT developer of IFMIS-Merger. FEMA has not adequately ensured that appropriate privileges granted to users are created, documented, and approved. We were informed by FEMA personnel that the system security functions are created and modified to provide additional functionality under specific menus in the IFMIS-Merger application. As a result, these changes to the menu provide additional functionality to the users with access to those menus. However, current documentation over IFMIS-Merger, including access authorization forms, change management plans and SSPs, do not define how to manage and document changes to these functions to ensure that approved changes are made and appropriate and traceable access is granted to IFMIS-Merger users. While FEMA has received the IFMIS Security Functions Reference Guide dated 2007 from the software vendor, we determined that the documentation is a technical reference	• Dedicate resources to assess the usage of IFMIS-Merger system security functions against DHS policy requirements and determine gaps that exist within existing system documentation over the security functions. • Develop and implement policies and procedures documenting the process of adding, deleting, and modifying IFMIS-Merger system security functions to ensure that proper controls are in place for approving, testing and documenting these functions prior to implementation, in accordance with DHS policy. These policies and procedures should include requirements over independent monitoring of the creation, modification and deletion of system security functions, and requirements for updating system documentation to reflect the impact of the changes to user account privileges. • Develop and implement procedures to ensure that functions updated through the change management process are formally approved and documented and that appropriate system documentation for IFMIS-Merger system security		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	manual that defines the capabilities of the system, usage of the various system security functions, menu options and related permissions for each function. However, the guide does not address the management of these system security functions from a change control and access control perspective for FEMA. Additionally, the guide does not include requirements for updating system documentation and tracking these system security function changes to privileges in the system. Consequently, based on our testwork, we concluded that a formalized process for modifying specific IFMIS-Merger system security functions to ensure that appropriate privileges are created, documented, approved, and monitored does not exist.	functions is updated and retained, in accordance with DHS policy.			
FEMA-IT-10-50	During the FY 2010 audit engagement, we determined that the following conditions related authorization of external connections to the FEMA VPN continue to exist: • Two-factor authentication is not used for VPN access, as required by DHS policy. • The existing documentation that defines the process for granting and maintaining VPN access to the FEMA network does not include requirements for administering the site survey process, including requirements for the authorization of the sites surveys, recertification of site surveys, and the security requirements associated with the various aspects of the process. • FEMA has not formally identified and documented the roles and responsibilities necessary within FEMA to properly authorize and administer VPN access to	• Implement and require two-factor authentication for all remote access to the FEMA network, as required by DHS policy and Federal Information Processing Standards (FIPS) 140-2. • 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. Specifically, clearly define and document a formalized process for the authorization, review, and maintenance of VPN access agreements between FEMA and external entities. Additionally, ensure that within the policies and procedures, appropriate roles and responsibilities over the process are defined to include authorizations by the CISO/Information System Security Manager (ISSM) to connect to		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	individuals using non-DHS equipment to access the FEMA network. • Access for state emergency management agencies and FEMA contractors to load the VPN client onto state or contractor owned equipment to connect to the FEMA LAN is approved by the SOC. However, DHS policy requires that any non-DHS equipment connecting to a DHS network must be authorized by the Component CISO/ISSM. • FEMA's *VPN Rules of Behavior for Users Behind Corporate Firewalls*, dated December 5, 2002, requires an Inter-Agency VPN Agreement between FEMA and external organizations before permitting VPN access to the FEMA network through non-Government issued equipment such as contractor or state agency workstations. However, we determined that Inter-Agency VPN Agreements have not been documented and that this requirement is inconsistent with DHS policy, which requires Interconnection Security Agreements (ISAs) or Memoranda of Understanding/Memoranda of Agreement (MOUs/MOAs) prior to establishing a VPN connection from equipment operating on an external network. • FEMA's approval of requests for network connections to external organizations through VPN access for remote users is based on security control information submitted by the external entities via site surveys. Based upon our review of existing site surveys and the site survey process, we noted that: • The site surveys do not contain the level of	non-DHS equipment. • Ensure that agreements related to VPN access are reviewed and recertified when a major system change occurs or every three years, in accordance with DHS policy. • Formally identify and document appropriate roles and responsibilities related to management of remote access to the FEMA network, including iPass and VPN. • Document and implement policies and procedures to ensure that formalized ISAs, MOUs, or MOAs, delineating security responsibilities by FEMA and external organizations when connecting through non-DHS equipment to the FEMA network via VPN access are used. Such agreements should include evidence of validation by FEMA management that security controls in place on external entity networks are appropriate and satisfy requirements for minimum security controls on DHS and FEMA systems prior to connection in accordance with DHS policy.			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	technical granularity describing the external network security controls required to appropriately approve a connection to the FEMA LAN, and the FEMA SOC does not independently verify the accuracy of information in the site surveys submitted by external entities prior to approving the connection and subsequently granting VPN access to users. • DHS guidance indicates that a single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. However, we determined that the security accreditation of the connecting networks is not being evaluated by the FEMA SOC during the review of site surveys to ensure the security requirements are appropriately implemented.				
FEMA-IT-10-51	In FY 2009, we identified weaknesses over configuration management controls related to NEMIS program libraries and directories within the Test and Development Laboratory (TDL) environment. During the FY 2010 audit, we determined that the following weaknesses continue to exist: • Controls to segregate access within the TDL environment have not been appropriately implemented. Specifically, IT Systems Integration personnel do not grant separate privileges to development code, which is moved to TDL by the systems developer, and pre-production code, which has completed User Acceptance Testing (UAT) and is pending deployment to the NEMIS production	• Document and implement formalized policies and procedures for restricting and monitoring access to the NEMIS TDL directories to ensure that the principles of least privilege and segregation of duties are enforced, in accordance with DHS guidance. The process should include requirements over periodic monitoring and documented reviews of NEMIS TDL directories to verify that no changes have occurred after the approval of NEMIS system changes. • Implement technical controls within the NEMIS TDL environment to limit developers' access to pre-production directories containing "locked" application code changes to "read only". If		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	environment. As a result, developers have read, write and execute privileges to all code in the TDL environment. • Code approved for implementation is not locked down within the TDL environment prior to deployment to production. Additionally, while an ad-hoc review is performed over the directories to monitor the modification dates on the production code directories, this process is not performed consistently or documented to mitigate the risk associated with not restricting access to the approved code.	business needs require that the segregation of duties cannot be immediately implemented, FEMA should document and implement policies and procedures to compensate for the risk associated with the segregation of duties weakness noted, in accordance with DHS guidance.			
FEMA-IT-10-52	Conditions noted in FY 2009 related to weaknesses over vulnerability assessments for the Windows server environment within the NFIP LAN supporting the Traverse application continue to exist in FY 2010. Specifically: • While procedures have been developed, the NFIP contractor has not fully implemented the process for conducting internal vulnerability scans for information systems and for assessing, reporting, and correcting identified weaknesses through the POA&M Process in accordance with FEMA and DHS guidance. • FEMA does not have documented and approved procedures that establish formal requirements, processes, and responsibilities for conducting monitoring and oversight of regular vulnerability scans performed over the NFIP LAN which supports Traverse to meet DHS vulnerability assessment requirements.	• Document and implement formal policies and procedures that outline the processes and requirements for performing internal vulnerability scans over all NFIP information systems as well as the process for assessing, reporting, and correcting weaknesses identified during scans as required by FEMA and DHS policy. • Ensure that policies and procedures formally designate responsibilities of FEMA OCIO and NFIP IT security management for the implementation, monitoring, and oversight of the vulnerability scanning process, so that the scope of vulnerability scans conducted include all NFIP workstations and servers and include requirements for formally tracking and monitoring the remediation of vulnerabilities identified during the internal scans of the NFIP LAN through the POA&M process, in accordance with DHS policy.		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Furthermore, while ad hoc scans were performed in previous years by the contractor, evidence of periodic NFIP network scanning conducted in FY 2010 could not be obtained. Additionally, we inquired with FEMA and determined that scans over the NFIP LAN supporting the Traverse application were not performed by the FEMA SOC.				
FEMA-IT-10-53	During our FY 2010 audit test work, we noted that NFIP has not established or implemented an effective process to periodically recertify user access, including service accounts, on the TRRP mainframe. Currently, NFIP requires users to sign security awareness and training certifications on an annual basis. However, no review of users' access and privileges is conducted by management on a periodic basis to ensure system access remains appropriate and commensurate with job responsibilities in accordance with DHS guidance. Additionally, we noted through inspection of the TRRP access procedures that no process has been established to formally document both the approval and business need for service accounts.	• Complete the revision, documentation, and full implementation of TRRP access control policies and procedures, and ensure that they include a formalized process for the recertification of all accounts on the mainframe, including service accounts, on an annual basis to determine that access remains appropriate and commensurate with job responsibilities in accordance with DHS policy. • Document and implement policies and procedures over the creation of service accounts to ensure that they are appropriately authorized and that a clear business need is established and documented justifying the creation and use of these types of accounts in accordance with DHS policy.		X	2
FEMA-IT-10-54	During the FY 2010 audit engagement, we determined that weaknesses existed in the implementation of DHS SELC requirements over the IFMIS-Merger Project. Specifically, throughout the lifecycle of the project, FEMA management did not adequately define and implement required elements of the DHS SELC process, including: • A detailed and comprehensive Project Tailoring Plan	Conduct and document a lessons learned report related to the IFMIS-Merger project per DHS SELC guidance. By conducting such an activity, FEMA management will be able to maintain a record of lessons learned in order to increase the probability of success for future acquisitions through the improvement of processes, tools, and other project related entities.	X		3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	to define required stages, activities, artifacts and exit criteria for the project per DHS SELC guidance was not developed and approved by FEMA management. • Approvals for project critical documentation demonstrating that all required stakeholders reviewed and approved the results before advancing to subsequent SELC stages could not be provided. • FEMA could not provide a Data Migration Plan and Test Strategy to demonstrate that critical DHS SELC requirements were documented and approved prior to implementation of the data migration. • System security requirements and milestones were not documented and integrated into key project documentation, such as Business Requirements documents, project schedules, Project Management Plans, and Risk Management Plans. • Project documentation including the Project Management Plan, the Risk Management Plan, and Business Requirements documents were not updated and revised throughout the project duration as required by the DHS SELC. • Key information such as roles and responsibilities of all stakeholders, guidelines for developing business requirements documentation, requirements for stage reviews, and key exit criteria before moving to the next stage of the project were not integrated into the project schedule, Project Plan, and Communications Plan. • FEMA management did not provide adequate	Additionally, we determined that the root cause associated with the weaknesses noted over the SELC process is related to the entity level control issue identified in FEMA-IT-10-47, FEMA Management Needs to Improve Planning, Management, and Communication Related to Financial Systems Development and Acquisition Projects. While the IFMIS-Merger project has been completed, corrective action over the establishment of a process to provide oversight to the implementation of the SELC methodology must be completed. Please see NFR FEMA-IT-10-47 for recommendations related to the establishment of this process.			

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	oversight of the contractors implementing the IFMIS-Merger Project. Specifically, documented evidence supporting the approval, validation, and retention of required artifacts associated with the data migration and other key project management documents could not be provided by FEMA or were insufficient based on DHS requirements.				
FEMA-IT-10-55	During our FY 2010 audit test work, we noted the following weaknesses related to the management and monitoring of user accounts and activity on the NFIP LAN supporting Traverse: • NFIP has not established or implemented a formal process to periodically recertify all accounts with access to the NFIP LAN supporting Traverse, as required by DHS and FEMA policy. Specifically, six system and/or service accounts on the FEMA LAN remained active absent an acceptable documented business need and justification. We were informed by NFIP management that these accounts were no longer needed, and they were removed from the system during test work. • Audit logs generated and reviewed on the NFIP LAN do not include changes to user account privileges as required by DHS and FEMA policy. • Audit logs for the NFIP LAN are not retained for at least 90 days, in accordance with DHS policy.	• Complete the revision, documentation, and full implementation of access control policies and the NFIP LAN system account management procedures to align with DHS requirements such as recertification of accounts and audit log reviews. Specifically, ensure that they include a formalized process for the recertification of all accounts on the NFIP LAN, including service accounts, on an annual basis to determine if access remains appropriate and commensurate with job responsibilities in accordance with DHS policy. • Document and implement policies and procedures over the creation of service accounts to ensure that they are appropriately authorized and that a clear business need is established and documented justifying the creation and use of these types of accounts in accordance with DHS policy. • Configure the NFIP LAN audit logs to include changes to user account privileges and ensure that storage capacity settings of audit logs are configured to retain the logs for 90 days online as	X		2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		required by DHS and FEMA policy.			
FEMA-IT-10-56	During our FY 2010 audit engagement, we noted the following weaknesses related to the monitoring of user accounts and activity on the TRRP mainframe: • Segregation of duties is not properly implemented over the review and maintenance of TRRP audit logs. Specifically, the TRRP system administrator is responsible for reviewing TRRP audit logs, and a second independent reviewer is not required. • Audit logs generated and reviewed on the TRRP mainframe do not include changes to user account privileges as required by DHS and FEMA policy.	• Develop and implement TRRP audit logging policies and procedures that include requirements for audit log configurations and the review of logs by IT security management independent of the system administration team in accordance with DHS policy. • Configure the TRRP audit logs to include changes to user account privileges as required by DHS and FEMA policy.	X		2
FEMA-IT-10-57	During our FY 2010 audit test work, we noted that NFIP has not established or implemented a formal process to authorize or periodically review remote access to the LAN hosting the TRRP mainframe environment in accordance with DHS and NIST guidance.	• Develop, document, and fully implement policies and procedures over documenting, reviewing, and approving remote access to the NFIP LAN hosting the TRRP mainframe environment in accordance with FEMA and DHS requirements. • Develop, document, and fully implement policies and procedures to perform a periodic recertification of all remote user access and retain auditable records as evidence that recertifications are conducted and completed in accordance with DHS and FEMA policy.	X		2
FEMA-IT-10-58	While improvements were noted over the documentation of Traverse change management procedures during the FY 2010 audit test work, we determined that certain weaknesses identified in FY 2009 continue to exist over the Traverse configuration management process in comprehensively addressing FEMA and DHS change	• Ensure the NFIP contractor continues to dedicate resources to establish and implement documented policies and procedures over the Traverse change management process for non-emergency and emergency changes which are in line with DHS configuration management requirements.		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	management policy. For example, we determined that: • Established procedures do not include guidance for initial approvals as we were informed that Traverse currently does not fall under review of the NFIP Change Control Board (CCB). • Requirements for managing the change management program have not been adequately established and implemented to ensure that NFIP CCB and/or Technical Review Committee (TRC) approvals are granted prior to implementing changes into the Traverse production environment, as required by FEMA and DHS policy. • Adequate oversight and involvement from FEMA management is not integrated into the configuration management requirements. Specifically, FEMA is not involved in testing and/or reviewing testing and approving changes to Traverse prior to implementation. • Traverse changes are not required to be tested prior to implementing the change into production as no testing environment exists. • Limited testing requirements exist to guide personnel in the development of test plans and guidance over the testing that should be performed and documented. Additionally, roles and responsibilities over test plan procedures to ensure that plans are sufficient, document expected outcomes, and are reviewed and approved prior to development, are not documented. • Requirements for Traverse emergency changes have not been formally defined.	Particular emphasis must be placed on approval by the NFIP CCB and/or TRC, initial change approvals, testing and testing requirements, final approvals, and retention of required change management artifacts to track all changes throughout their lifecycle. These phases should also include an integrated process to address system change requirements and stakeholder change requirements to ensure adequate testing and approvals are completed by the appropriate parties. • Establish and implement a formal process to conduct user acceptance testing in a test environment prior to implementation in production. • Allocate qualified NFIP management and OCIO IT security resources to provide adequate oversight for the configuration management process. Oversight activities should encompass requirements such as a NFIP Program Configuration Management Board responsible for managing and participating in the NFIP CCB and/or TRC to ensure that all required elements in the configuration management process are formally defined and implemented in accordance with DHS and FEMA guidance. • Dedicate the resources to fully review and finalize approval of all NFIP contractor's configuration management policies and procedures to ensure the revised procedures are compliant with DHS requirements.			

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

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

FEMA-IT-10-59	While improvements were noted over the documentation of TRRP change management procedures during the FY 2010 audit test work, we determined that certain weaknesses identified in FY 2009 continue to exist over the TRRP configuration management process in comprehensively addressing FEMA and DHS change management policy. For example, we determined that:
	• Requirements for managing the change management program have not been adequately established and implemented to ensure that CCB and/or TRC approvals are granted prior to implementing changes into the TRRP production environment, as required by FEMA and DHS policy. Specifically:
	  • While a CCB has been established by NFIP management, adequate oversight and involvement from FEMA management has not been integrated into the configuration management requirements including mandatory FEMA participation in the CCB and CCB approval of changes after testing has occurred.
	  • FEMA management, including IT security and financial personnel, are not involved in testing and/or reviewing testing and approving changes to TRRP prior to implementation.
	  • CCB reviews are not conducted for approval of final changes prior to implementation into production as required by FEMA and DHS guidance.
	• Limited testing requirements exist to guide personnel in the development of test plans and guidance over the
		• Ensure the NFIP contractor continues to dedicate resources to establish and implement documented policies and procedures over the TRRP change management process for non-emergency and emergency changes which are in line with DHS configuration management requirements. Particular emphasis must be placed on initial change approvals, testing and testing requirements, final approvals, and retention of required change management artifacts to track all changes throughout their lifecycle. These phases should also include an integrated process to address system change requirements and stakeholder change requirements to ensure adequate testing and approvals are completed by the appropriate parties.
		• Allocate qualified NFIP management and OCIO IT security resources to provide adequate oversight for the configuration management process. Oversight activities should encompass requirements such as a NFIP Program Configuration Management Board responsible for managing and participating in the NFIP CCB and/or TRC to ensure that all required elements in the configuration management process are formally defined and implemented in accordance with DHS and FEMA guidance.
		• Dedicate the resources to fully review and finalize approval of all NFIP contractor's configuration management policies and procedures to ensure the revised procedures are compliant with DHS requirements.
				X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	testing, including user acceptance testing, that should be performed and documented prior to approval and implementation into production. Additionally, roles and responsibilities over test plan procedures to ensure that plans are sufficient, document expected outcomes, and are reviewed and approved prior to development, are not documented. • Requirements for TRRP emergency changes have not been formally defined in writing. Furthermore, we performed testwork over initial and final approvals for a selection of 25 TRRP changes made in FY 2010 and noted the following exceptions: • Documentation for 3 of the 25 changes could not be provided • 17 of 22 changes tested did not have initial approvals documented prior to developing the change • 9 of 22 changes tested changes did not have all the required approvals prior to implementation • 1 of 22 changes tested was implemented prior to change documentation being completed				
FEMA-IT-10-60	Weaknesses identified in FY 2009 related to controls to restrict access and control movement of Traverse program libraries and data continue to exist in FY 2010. Specifically: • Implementation procedures over Traverse changes have not been established, and current processes do	• In accordance with policy, enforce requirements over individual user accounts by not allowing vendors to a use a system administrator's account to access the system and deploy changes into production. • Document and implement policies and procedures		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	not incorporate segregation of duties requirements. Specifically, NFIP IT contractors use their individually assigned system administrator accounts to logon and create sessions to allow a third-party development vendor to install Traverse system changes. • NFIP does not have a formal process for monitoring changes that the vendor makes in Traverse while logged in as an administrator.	to limit Traverse developer and application support vendor access to the NFIP production environment to "read only" through an assigned user account and segregate the responsibility for deploying application code changes into production from the development/support vendor to an independent control group. Additionally, procedures should include implementation process requirements for controlling access to production directories. If business needs require that the segregation of duties cannot be immediately implemented, FEMA should document and implement policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance, including a formalized process for performing and documenting reviews of activity performed by third-party vendors within the Traverse environment.			
FEMA-IT-10-61	As noted during the FY 2009 audit engagement, weaknesses over contingency planning for both the Traverse and TRRP systems continue to exist in FY 2010. Specifically: • While the NFIP/LSS Contingency Plan, which pertains to the contingency planning around Traverse and the NFIP LAN, has been updated for FY 2010, the following elements are not in compliance with DHS and NIST requirements: • The NFIP/LSS IT Contingency Plan does not document detailed instructions for restoring	• Develop, document, and fully implement an IT Contingency Plan for NFIP components, including TRRP and Traverse. Additionally, ensure that contingency planning documentation includes detailed instructions for restoring operating system software and critical applications in the event of a disaster, contingency, or disruption of service in accordance with DHS and NIST policy requirements for systems categorized at the high impact availability objective. • Conduct and document annual tests of the TRRP		X	2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	operating systems and critical applications in the event of a disaster, contingency, or disruption of service. • The NFIP/LSS IT Contingency Plan does not designate the current alternate processing facility for the operating environment. • Testing of the NFIP/LSS IT Contingency Plan has not been performed in the 12 months, as required by DHS policy. • FEMA and NFIP management have not documented or approved a current IT Contingency Plan for the mainframe environment supporting the TRRP system in accordance with FEMA and DHS requirements. • Contingency testing over TRRP was not sufficiently conducted in accordance with DHS and NIST requirements. While a limited disaster recovery test of the NFIP mainframe environment, including TRRP, was performed in October 2009 to test restoration of data, all elements required to be tested under the DHS requirements for an IT Contingency Plan were not sufficiently addressed and could not be used to validate the effectiveness of the organization's contingency planning controls. • The NFIP contractor's COOP for Traverse and TRRP could not be provided for auditor review.	and Traverse IT Contingency Plan(s) that address all critical phases of the plan(s), and update contingency planning documentation with lessons learned, as necessary and in accordance with DHS and NIST requirements. • Dedicate resources to establish and implement an alternate processing site for the NFIP systems in accordance with DHS policy requirements. • Until an alternate processing site is established, develop and submit an exception for approval in accordance with DHS policy, and ensure that compensating controls over the lack of an alternate processing site have been implemented and are effective, and documentation of their effectiveness is maintained as auditable records. • Document, implement, and maintain the NFIP COOP to ensure required elements for Traverse and TRRP are included in accordance with DHS guidance for high impact systems.			
FEMA-IT-10-62	Conditions noted in FY 2009 related to weaknesses over the NEMIS configuration management process continue to exist in FY 2010. Based on our testwork, we concluded that NEMIS configuration management is not adequately	• Document and establish a centralized and integrated change management process over NEMIS to ensure that adequate controls are implemented throughout the lifecycle of the		X	3

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	and centrally controlled, documented, or managed throughout the lifecycle of the FEMA configuration management process. Specifically, we identified the following weaknesses: • NEMIS configuration management policy and procedures which outline FEMA's responsibilities and processes for initiating, monitoring, testing, and approving NEMIS non-emergency and emergency changes that are developed under the various development contracts have not been documented and approved by FEMA management, in accordance with DHS and FEMA policy. • FEMA does not have a centralized program management function or process to monitor and track NEMIS SCRs throughout the configuration management lifecycle, from initial approval through implementation into the production environment.	configuration management process, in accordance with DHS and FEMA policy. • Formally designate FEMA management responsibilities for oversight and implementation of controls for initiating, monitoring, testing, and approving all NEMIS non-emergency and emergency changes; • Establish a centralized, formal process to monitor, document, and track NEMIS software changes throughout the configuration management lifecycle, from initial approval through implementation into the production environment.			
FEMA-IT-10-63	During the FY 2010 audit engagement, we noted weaknesses over the IFMIS-Merger Configuration Management Plan (CMP). Based on our testwork, we concluded that the IFMIS configuration management process does not meet comprehensive change management process requirements and procedures as required by DHS and NIST guidance because it is not adequately documented. For example, we identified the following weaknesses: • The IFMIS CMP provided in July 2010 is in draft and has not been updated to reflect the new IFMIS-Merger operating environment. Specifically, the plan includes Core IFMIS and G&T IFMIS, but does not address the IFMIS-Merger instance that began operations in	• Revise, document and fully implement a comprehensive configuration management program that includes a Configuration Management Plan for IFMIS-Merger, which aligns with all applicable DHS and FEMA requirements and reflects the current IFMIS-Merger operating environment and all applicable IT components. • Include in policies and procedures (a) clearly defined and formalized responsibilities for change management oversight bodies including a Configuration/Change Control Board and (b) sufficiently detailed responsibilities and	X		2

NFR No.	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	February 2010. • Infrastructure information for the in-scope applications does not include the server information for G&T IFMIS, which was operational when the plan was last revised in November 2009. • The CCB has not been formally and fully integrated into the FEMA change management process. While we were informed that a CCB for IFMIS was established on March 22, 2010, we determined that the requirements over the roles and responsibilities as well as the membership of the CCB were not clearly defined, implemented, and documented to ensure that DHS requirements are met. • Membership of the "SCR Review Team" responsible for initial approval for development of any changes to the application is not formally defined. • Requirements that security impact analyses be performed prior to implementation of changes have not been documented. • Limited testing requirements exist to guide FEMA personnel in the development of test plans and guidance over the testing that should be performed and documented. Additionally, roles and responsibilities over test plan procedures to ensure that plans are sufficient, document expected outcomes, and are reviewed and approved prior to development, are not documented. • Requirements over emergency changes have not been defined in writing.	requirements for security impact analyses, test plan development, and approval for non-emergency and emergency change procedures.			

APPENDIX C

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

Current Year Notices of Findings and Recommendations at the Federal Emergency Management Agency

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
FEMA-IT-09-02	Configuration Management Weaknesses on IFMIS, NEMIS, and Key Support Servers (vulnerability assessment finding)		FEMA-IT-10-41
FEMA-IT-09-03	Weaknesses Exist over Recertification of Access to IFMIS		FEMA-IT-10-14
FEMA-IT-09-06	Documentation Supporting the IFMIS User Functions Does Not Exist		FEMA-IT-10-49
FEMA-IT-09-12	NEMIS Access Controls Need Improvement		FEMA-IT-10-01
FEMA-IT-09-13	Employee Termination Process for Removing System Access Should be More Proactive		FEMA-IT-10-21
FEMA-IT-09-17	System Programmers Have the Ability to Migrate Code into the IFMIS Production Environment		FEMA-IT-10-39
FEMA-IT-09-19	Monitoring of NEMIS System Software Needs Improvement		FEMA-IT-10-04
FEMA-IT-09-22	Alternate Processing Site for NEMIS Has Not Been Established		FEMA-IT-10-02
FEMA-IT-09-24	NEMIS Backups are Not Tested in Accordance with Policy		FEMA-IT-10-36
FEMA-IT-09-25	The NEMIS Contingency Plan is Not Tested		FEMA-IT-10-20
FEMA-IT-09-28	NEMIS Configuration Management Process for Non-Emergency Changes Needs Improvement		FEMA-IT-10-62
FEMA-IT-09-29	NEMIS Emergency Change Process Needs Improvement		FEMA-IT-10-62
FEMA-IT-09-38	Segregation of Duties Not Enforced for Traverse	X	
FEMA-IT-09-39	Traverse Contingency Plan Not Tested and NFIP Disaster Recovery and COOP Needs Improvement		FEMA-IT-10-61
FEMA-IT-09-45	IFMIS User Access is not Managed in Accordance with Account Management Procedures		FEMA-IT-10-26
FEMA-IT-09-46	IFMIS System Interconnections Agreements Have Not Been Reauthorized	X	
FEMA-IT-09-48	Corrective Action over NEMIS Vulnerabilities is Not Formally Documented		FEMA-IT-10-33
FEMA-IT-09-50	Weaknesses Exist over IFMIS Application and Database Audit Logging		FEMA-IT-10-11
FEMA-IT-09-51	NEMIS Oracle Audit Logging is Not Tracked		FEMA-IT-10-09
FEMA-IT-09-52	Existing NEMIS Patch Management Guidance Needs to be Implemented		FEMA-IT-10-35
FEMA-IT-09-53	The NEMIS SSP Had Not Been Fully Updated in Accordance with DHS Policy		FEMA-IT-10-18
FEMA-IT-09-54	Traverse Application Management Needs Improvement		FEMA-IT-10-58
FEMA-IT-09-56	G&T IFMIS Oracle Database Security Controls are Not Configured Properly		FEMA-IT-10-27
FEMA-IT-09-57	G&T IFMIS Oracle Database Auditing is Not Sufficient		FEMA-IT-10-13
FEMA-IT-09-58	Recertification of G&T IFMIS Application and Database Access has Not Been Performed		FEMA-IT-10-15
FEMA-IT-09-59	System Programmers Have the Ability to Migrate Code into the G&T IFMIS Production Environment		FEMA-IT-10-40
FEMA-IT-09-60	NFIP Legacy System C&A is Expired		FEMA-IT-10-24
FEMA-IT-09-61	G&T IFMIS Certification & Accreditation has Not Been Performed		FEMA-IT-10-16
FEMA-IT-09-62	VPN Remote Access is Not Appropriately Authorized or Monitored		FEMA-IT-10-25
FEMA-IT-09-63	External Connections to the FEMA VPN are Not Appropriately Authorized or Documented		FEMA-IT-10-50

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
FEMA-IT-09-64	Core IFMIS Oracle Database is Not Configured to Prevent the Reuse of Passwords		FEMA-IT-10-07
FEMA-IT-09-65	G&T IFMIS Access Authorizations are Not Consistently Documented		FEMA-IT-10-12
FEMA-IT-09-66	NEMIS Oracle Database is Not Configured to Enforce DHS Password Requirements		FEMA-IT-10-06
FEMA-IT-09-67	End-User Workstation Screensaver Configuration is Not Sufficient		FEMA-IT-10-03
FEMA-IT-09-68	PARS Has Not Been Certified and Accredited		FEMA-IT-10-29
FEMA-IT-09-69	Transaction Recording and Reporting Processing TRRP Configuration Management Plan Weaknesses		FEMA-IT-10-59
FEMA-IT-09-70	Traverse and the NFIP LAN Configuration Patch Management Weaknesses		FEMA-IT-10-23
FEMA-IT-09-71	Physical Security and Security Awareness Issues Were Identified During Enhanced Security Testing		FEMA-IT-10-38
FEMA-IT-09-72	Exception Request over IFMIS Audit Logging is Inconsistent with Existing Controls	X	
FEMA-IT-09-73	Core and G&T IFMIS System Software Administrator Activity is Not Appropriately Monitored		FEMA-IT-10-44
FEMA-IT-09-74	The FEMA Systems Inventory is Incomplete	X	
FEMA-IT-09-75	Requirements for Recertification of Access to the NFIP Data Center	X	
FEMA-IT-09-76	Emergency and Temporary Access to the Core IFMIS Database is Not Properly Authorized and Conflicts with Segregation of Duties Principles		FEMA-IT-10-30
FEMA-IT-09-77	FEMA and NFIP Planning, Management and Communication Related to Financial Systems Development and Acquisition Projects Needs to be Improved		FEMA-IT- FEMA-IT-10-47
FEMA-IT-09-78	Weaknesses Exist in the NEMIS Configuration Management Process under the Enterprise Applications Development Integration and Sustainment (EADIS) contract		FEMA-IT-10-62
FEMA-IT-09-79	Weaknesses Exist over Management of FEMA LAN Accounts		FEMA-IT-10-22
FEMA-IT-09-80	Vulnerability Assessments of the NFIP LAN is Inadequate		FEMA-IT-10-52
FEMA-IT-09-81	Improvements are Needed in Core and G&T IFMIS Internal Scanning Procedures and Processes		FEMA-IT-10-34
FEMA-IT-09-82	Core and G&T IFMIS Patch Management Weaknesses		FEMA-IT-10-32
FEMA-IT-09-83	EADIS NEMIS Access Restrictions to Program Directories Needs Improvement		FEMA-IT-10-51
FEMA-IT-09-84	PARS Database Security Controls are Not Appropriately Established		FEMA-IT-10-05
FEMA-IT-09-85	TRRP Password Configurations Have Not Been Configured in Accordance with DHS Policy	X	
FEMA-IT-09-86	Weaknesses Exist over the Implementation of Traverse System Changes		FEMA-IT-10-60
FEMA-IT-09-87	Weaknesses Exist in FEMA's Incident Response Program		FEMA-IT-10-31
FEMA-IT-09-88	Weaknesses Exist over Access Authorizations for TRRP		FEMA-IT-10-53
FEMA-IT-09-89	Weaknesses Exist over FEMA Background Investigations for Federal Employees and Contractors		FEMA-IT-10-45
FEMA-IT-09-90	FEMA LAN Certification and Accreditation Package is not Adequate		FEMA-IT-10-28
FEMA-IT-09-91	FEMA Contractor Tracking Program is Inadequate		FEMA-IT-10-10

U.S. Department of Homeland Security
Washington, D.C. 20472

FEMA

FEB 2 8 2011

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

THROUGH: Brad Shefka
Chief, FEMA GAO/OIG Liaison

FROM: Jean A. Etzel
Chief Information Officer/Director
Office of the Chief Information Officer

SUBJECT: Response to Draft Audit Report – *Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2010 DHS Financial Statement Audit – For Official Use Only OIG Project No.: 11-002-ITA-FEMA dated February 2011*

The Federal Emergency Management Agency (FEMA) appreciates the Department of Homeland Security (DHS) Office of the Inspector General providing KPMG's evaluation of FEMA's information technology (IT) general controls and their recommendations for improving FEMA's financial processing environment and related IT infrastructure. The evaluation has been very helpful in identifying areas requiring improvement and prioritizing work to implement their recommendations.

Generally FEMA concurs with the auditor's recommendations in the report referenced above. The Chief Information Officer (CIO) is resolute in directing these audit recommendations be effectively implemented in a timely manner. Weekly, FEMA's Audit Remediation Team meets with the Action Officers to review the status of implementing these recommendations and address issues that are impeding progress. Branch Chiefs receive weekly reports reflecting the current status of their organization's assigned actions and are working diligently to correct findings and implement recommendations. Implementation of corrective actions is a performance goal for each Branch Chief in the Office of the Chief Information Officer.

In addition to the detailed Plan of Action and Milestones (POA&M) for each audit recommendation in the DHS Trusted Agent FISMA (TAF) system, FEMA has developed detailed remediation work plans to ensure root causes are addressed. Remediation work plan status is discussed at weekly meetings with senior management. If you have any questions regarding the status of the planned actions, we are available to meet with your office. FEMA's senior leadership is committed to completing the remaining actions included in each of the POA&Ms at the earliest possible time.

If you have any questions, please have your staff contact Deborah Moradi, Chief, Governance and Investment Integration Branch, at 202-646-3154.

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 Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of 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 visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

• Call our Hotline at 1-800-323-8603;

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

• Email us at DHSOIGHOTLINE@dhs.gov; or

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

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