Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2009 DHS Integrated Audit

OIG-10-92

May 2010

Office of Inspector General

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

May 28, 2010

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 component of the FY 2009 DHS financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors Report* dated November 13, 2009 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at FEMA in support of the DHS FY 2009 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 5, 2010, 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

March 5, 2010

Inspector General
U.S. Department of Homeland Security
Chief Information Officer
Federal Emergency Management Agency
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, 2009 and the related statement of custodial activity for the year then ended (referred to herein as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting (ICOFR) of the balance sheet as of September 30, 2009, and 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, for the year ended September 30, 2009 (referred to herein as "other fiscal year [FY] 2009 financial statements"), or to examine ICOFR over the other FY 2009 financial statements. Because of matters discussed in our *Independent Auditors' Report*, dated November 13, 2009, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements. In addition, we were unable to perform procedures necessary to form an opinion on DHS' ICOFR of the FY 2009 balance sheet and statement of custodial activity.

In connection with our FY 2009 engagement, we examined the Federal Emergency Management Agency's (FEMA) internal control over financial reporting by obtaining an understanding of FEMA's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls. As noted above, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the effectiveness of ICOFR. Further, other matters involving ICOFR may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheet as of September 30, 2009, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other FY 2009 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 over financial reporting 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 over financial reporting, 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.

During our audit engagement, we noted certain matters in the areas of security management, access controls, configuration management, and contingency planning with respect to FEMA's financial systems information technology (IT) general controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. These matters are described in the *IT General Control and Financial System Functionality Findings by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 13, 2009. This letter represents the separate restricted distribution report mentioned in that report.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also described in the *IT General Control and Financial System Functionality Findings by Audit Area* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and are intended. We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. In addition, we have provided the following: a description of key FEMA financial systems and IT infrastructure within the scope of the FY 2009 DHS financial statement audit engagement in Appendix A; a description of each control deficiency in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Acting Chief Financial Officer dated December 09, 2009.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General, the 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, 2009

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

During our engagement to perform an integrated audit of Department of Homeland Security (DHS or the Department), we evaluated the effectiveness of information technology (IT) general controls of DHS' financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit procedures as they relate to our IT general control assessment at the Federal Emergency Management Agency (FEMA). The scope of the FEMA IT general controls assessment is 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 statement 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 IT general 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 and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Segregation of Duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our IT general controls audit procedures, we also performed technical security testing for key network and system devices. The technical security testing was performed from within a select FEMA facility, and focused on test, development, and production devices that directly support FEMA's financial processing and key general support systems. Limited social engineering and after-hours physical security testing was also included in the scope of technical security testing.

In addition to testing FEMA's IT general control environment, we performed testing of automated application controls on a limited number of FEMA's financial systems and applications. 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* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2009, FEMA took corrective action to address certain prior year IT control weaknesses. For example, FEMA made improvements by finalizing and executing agreements for interconnections with external Federal agencies, developed and implemented financial system backup procedures, made incremental progress in improving processes for recertifying financial application user accounts, and improved the process for retaining National Flood Insurance Program (NFIP) change control documentation. However, during FY 2009, we continued to identify IT general control deficiencies at FEMA. The most significant deficiencies from a financial statement audit perspective related to controls over security management, access to programs and data, program changes, and contingency planning. Collectively, the identified IT control weaknesses limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted internal control over FEMA's financial reporting and its operation, and we consider them to collectively represent a material weakness for FEMA under standards established by the American Institute of Certified Public Accountants (AICPA). In addition, based upon the results of our test work, we noted that the FEMA did not fully comply with the Department's requirements under the *Federal Financial Management Improvement Act of 1996* (FFMIA).

Of the 58 findings identified during our FY 2009 testing, 22 were repeat findings, either partially or in whole from the prior year, and 36 were new IT findings. These findings represent deficiencies in each of the five FISCAM control areas. We also considered the effects of financial systems functionality when testing internal controls since key FEMA financial systems are not compliant with FFMIA and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic control deficiencies and strengthening the control environment at FEMA.

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 and databases and supervisor re-certifications 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 and configuration 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 tested contingency plans. These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and FEMA financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS consolidated financial statements.

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

IT GENERAL CONTROL AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS BY AUDIT AREA

Findings Contributing to a Material Weakness in IT at the Department Level

Conditions: In FY 2009, the following IT general control deficiencies were identified at FEMA and contributed to a DHS-level significant deficiency that is considered a material weakness in IT general controls.

1. Security Management – we noted:
    - The Grants and Training (G&T) Integrated Financial Management Information System (IFMIS) and the Payment and Reporting System (PARS) were not certified and accredited prior to implementation into the production environment in FY 2007 and had been operating without an Authorization to Operate (ATO);
    - Information System Security Officers (ISSO) and Designated Authorizing Authority (DAA) were not formally designated for G&T IFMIS and PARS;
    - Vulnerabilities identified during periodic internal scans of the National Emergency Information System (NEMIS) and related corrective actions were not reported and tracked in accordance with DHS policy;
    - G&T IFMIS and PARS were not included in FEMA's systems inventory, and neither system was being tracked via the Trusted Agent Federal Information Security Management Act repository; and
    - The FEMA Switch Network (FSN)-2 certification and accreditation (C&A) package did not include the Maryland (MD) National Processing Service Center (NPSC) local area network (LAN) subsystem on which the primary servers for FEMA financial applications reside, and security roles for the MD NPSC were not formally designated.
2. Access Controls – we noted:
    - Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting the key financial applications and general support systems;
    - Core IFMIS, G&T IFMIS, NEMIS, and PARS application and/or database accounts, network, and remote user accounts were not periodically reviewed for appropriateness, 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;
    - Financial application, network, and remote user accounts were not disabled or removed promptly upon personnel termination;
    - Initial and modified access granted to Core and G&T IFMIS financial application and/or database, network, and remote users was not properly documented and authorized;

- Documented procedures for auditing NEMIS, Core IFMIS, G&T IFMIS, and PARS databases do not meet DHS requirements. Additionally, for these financial systems, logging of application and/or database events required to be recorded was not enabled, audit logs were not 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 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 does 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 DHS Waivers and Exceptions Request Form related to Core IFMIS financial database audit logging deficiencies was approved based on inconsistently or inaccurately described mitigating and compensating security controls over the financial application and database, and controls required as a condition of DHS approval were not implemented;
- System administrator root access to one instance of IFMIS was not properly restricted, logged, and monitored; and
- Emergency and temporary access to the Core IFMIS, G&T IFMIS, and PARS databases were not properly authorized, and contractor development personnel were granted conflicting access to implement database changes.

3. Configuration Management – we noted:

- 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 are within scope. Additionally, there was no application or tool in place to support the audit logging function on the NEMIS servers;
- Implemented emergency and non-emergency changes to NEMIS system software were not consistently documented, tested, approved, controlled, tracked, and retained on file;
- G&T IFMIS contracted developers/programmers were granted unrestricted access to the production environment through the "ifmiscm" account, which is used to deploy changes into production;
- A finalized patch management policy that includes the timeframe for installing patches was not implemented for financial systems; and
- Access was inappropriately granted to NEMIS developers to allow unrestricted access to both the production and development environments, and code in the NEMIS server directory environment is not locked down to prevent access to the Test and Development Laboratory and production environments after the code is approved for implementation.

4. Contingency Planning – we noted:

   - An alternate processing site for NEMIS was not established and implemented. Additionally, the approved DHS waiver was expired, and documented controls for restoring NEMIS servers from backup tapes to compensate for the lack of an alternate processing site were ineffective.

Recommendations: We recommend that the FEMA Chief Information Officer (CIO), FEMA Chief Financial Officer (CFO), and other relevant FEMA management, in coordination with the DHS CIO and Acting CFO, make the following improvements to FEMA's financial management systems and associated IT security program:

1. For Security Management:

   - Certify and accredit G&T IFMIS and PARS in accordance with applicable DHS policies and Federal guidance;
   - Formally designate ISSOs and DAAs for G&T IFMIS and PARS;
   - Develop and implement procedures that outline the process for formally reporting and tracking resolution of weaknesses identified during NEMIS internal vulnerability scans in accordance with DHS guidance;
   - Update the FEMA systems inventory to include G&T IFMIS and PARS and consistently adhere to policies and procedures for updating and monitoring the systems inventory to ensure that all new and current systems are accounted for with complete and accurate information, in accordance with NIST and DHS policy; and
   - Conduct a risk assessment of the MD NPSC LAN that supports FEMA financial systems, and review and revise the FSN-2 C&A package to reflect the current environment and include the MD NPSC LAN. Additionally, formally designate an ISSO and DAA for the MD NPSC.

2. 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. 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 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 Core IFMIS and G&T IFMIS database and financial application logs and the maintenance of documentation supporting such reviews in accordance with DHS requirements;
- 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;
- Configure NEMIS 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;
- Submit a revised DHS Waivers and Exceptions Request Form that accurately reflects the mitigating and compensating controls in place on the Core IFMIS financial application and database that justify exception from DHS audit logging policy. Additionally, ensure that (1) future requests include input from system owners and administrators to help ensure risk mitigation strategies accurately reflect implemented security controls and (2) a more formal process is established for providing and communicating approved waivers and conditions of approval to system owners;
- 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 Core IFMIS, G&T IFMIS, and PARS emergency and temporary database access that includes segregation of duties considerations and appropriate approval from FEMA management.

3. For Configuration Management:

- 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 configuration management policies and procedures for NEMIS emergency and non-emergency changes to financial system applications software, and ensure consistent adherence with requirements for approving, testing, documenting, properly controlling and tracking changes, and retaining related documentation;
- Limit the contracted developers/programmers' access to the G&T IFMIS production environment to "read only," and segregate the responsibility for deploying application code changes into

production from the contractor to an independent control group. If business need does not allow for segregation of these duties, FEMA should document policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance;

- Dedicate the appropriate resources to complete efforts to document, finalize, and implement comprehensive patch management policies and procedures, including requirements for timely implementation of required patches; and
- Develop and implement formal processes and procedures for restricting and monitoring access to the NEMIS production directories to ensure that the principles of least privilege and segregation of duties are enforced. The process should include requirements over the monitoring of NEMIS system directories to ensure that no changes have occurred after the approval of NEMIS system changes has occurred. Additionally, FEMA should limit developers' access to the NEMIS production directories to "read only" and segregate the responsibility for delivering application code changes into the NEMIS directory server from the contractor to an independent control group.

4. For Contingency Planning:
   - Complete on-going efforts to establish and implement an alternate processing site for NEMIS. Until an alternate processing site is established, obtain a current waiver approved by DHS and ensure that identified compensating controls are operating effectively to address the lack of an alternate processing site.

Other Findings in IT General Controls

Conditions: Although not considered to be a material weakness, we also noted the following other matters related to IT control deficiencies during the FY 2009 IT audit procedures at FEMA:

1. Security Management – we noted:
   - The revised system security plan (SSP) for NEMIS did not fully document the systems boundaries, define all subsystems and major applications, or establish security responsibilities for all system components;
   - The C&A for the legacy National Flood Insurance Program (NFIP) IT system pertaining to the Traverse application, Transaction Recording and Reporting Processing (TRRP) application, and NFIP LAN was expired, and the system was operating without a current ATO;
   - For the majority of FY 2009, a finalized and executed Memorandum of Understanding and an Interconnection Sharing Agreement was not in place between FEMA and the Department of the Treasury. *(Note: This issue was fully remediated during the audit and no further recommendation was required.)*;
   - Procedures for managing IT security incidents were not developed, approved, and implemented, and our unannounced vulnerability assessment scanning activity was not detected and appropriately reported by FEMA IT, in accordance with DHS and FEMA incident response policy;

- FEMA Office of the Chief Financial Officer (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 Office of the Chief Information Officer (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;
- Suitability investigations for FEMA federal employees and contractors were not appropriately conducted, and position designations 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; and
- FEMA did not have a process for tracking the status of contractors or an effective and formal process for notifying the OCIO of changes in contractor status so that user accounts could be appropriately disabled, removed, or modified in a timely manner.

2. Access Controls – we noted:

   - A formalized process did not exist to guide Core IFMIS staff in the modification of system accounts to ensure that appropriate privileges were created, documented, and approved for a specific security function, and the use of function modification privileges was not monitored;
   - The Core IFMIS database and TRRP system were configured with weak passwords that did not comply with DHS policy. (*Note: TRRP password settings were reconfigured during the audit to exceed DHS requirements. The weakness was fully remedied and no further recommendation was required.)*;
   - FEMA end-user workstations were not properly configured to activate a password-protected screensaver after 5 minutes of inactivity, as required by DHS policy;
   - Policies and procedures that require periodic documented recertification of NFIP data center access at a defined frequency were not developed and implemented; and
   - Processes to formally document authorizations, approvals, business needs, and recertification of TRRP system service accounts were not established. As a result, evidence that service accounts were authorized was not on file, and service accounts were not included in TRRP recertification efforts.

   We also identified exceptions related to access controls during our after-hours physical security testing. Details of the exceptions identified are outlined in the *After-Hours Physical Security Testing* section of this report.

3. Configuration Management – we noted:

   - Formal procedures were not implemented to require monitoring of developers' changes to Core IFMIS directories and sub-directories to financial applications to review and validate implemented changes, and informal reviews of developer activities were not routinely performed and documented;

- The configuration management plans for the NFIP Traverse and TRRP systems did not comprehensively provide guidance to address all configuration management control elements required by FEMA and DHS policy;
- TRRP changes were not approved prior to development and implementation into production;
- Procedures for approving, testing, and ensuring timely installation of operating system patches for the NFIP LAN, Traverse, Core IFMIS, and G&T IFMIS were not developed and implemented;
- Formal procedures for conducting internal scans of the Core IFMIS, G&T IFMIS, and NFIP LAN and Traverse operating system were not developed, remediation of vulnerabilities identified during internal scans were not tracked and monitored, and certain workstations were excluded from the scope of NFIP LAN scans conducted; and
- 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.

4. Segregation of Duties – we noted:
   - Incompatible duties that must remain segregated when granting and maintaining Traverse user access and processes for segregating incompatible duties within Traverse were not formally documented in existing policies and procedures.
5. Contingency Planning – we noted:
   - NEMIS backup tapes were not regularly tested in accordance with 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. Additionally, the waiver approved by DHS that identified table-top testing as a compensating control for FEMA's inability to fully test NEMIS was expired; and
   - The existing TRRP and Traverse contingency plans and NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan were not current or tested for systems recovery and failover capability at the alternate processing site. Additionally, the Traverse and TRRP alternate processing facility and TRRP critical data files were not documented in the existing disaster recovery and continuity of operations plan.

Recommendations: We recommend that the FEMA CIO, FEMA CFO, and other appropriate FEMA management, in coordination with the DHS CIO and Acting CFO, make the following improvements to FEMA's financial management systems:

1. For Security Management:
   - 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;
   - Complete the recertification and accreditation of the NFIP legacy system and re-authorize the system for operation, in accordance with DHS policies and Federal guidance;

- 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 System Engineering Life Cycle and acquisition requirements and Federal guidance;
- 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 contracting personnel, in accordance with DHS policy; and
- Document and implement procedures for tracking contract 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.

2. For Access Controls:

- Develop and implement policies and procedures that document the process of adding, deleting, and modifying Core IFMIS 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;
- Reconfigure Core IFMIS database passwords to enforce full compliance with DHS policy;
- Configure the FEMA LAN domain security policy to automatically activate password-protected screensavers on end-user workstations after the period of inactivity defined in DHS policy;
- Develop and implement policies and procedures for periodic recertification of physical access to the NFIP data center, to include the required frequency of reviews and the documentation that should be maintained as evidence of reviews conducted; and
- Revise the TRRP access control policies and procedures to ensure that the creation of service accounts are appropriately authorized and that a clear business need is established and documented. Additionally, ensure that policies and procedures over TRRP access authorization include the recertification of service accounts in accordance with DHS policy.

3. For Configuration Management:

- Develop and implement formal procedures for conducting periodic reviews of Core IFMIS 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;

- Update the current versions of NFIP Traverse and TRRP configuration management procedures to comprehensively address DHS and FEMA requirements, including requirements to initially approve changes prior to development and implementation in the production environment;
- Ensure the implementation of an updated version of the current TRRP configuration management procedures that comprehensively addresses requirements. 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 changes into production;
- Document, finalize, and implement comprehensive patch management policies and procedures that outline requirements for authorizing, testing, and installing required NFIP LAN, Traverse, Core IFMIS, and G&T IFMIS operating system patches. The policies and procedures should establish timeframes for installing required patches;
- Develop, finalize, and implement formal procedures over Core and G&T IFMIS and the NFIP LAN and Traverse operating system for: (1) conducting periodic internal vulnerability scans of FEMA and NFIP financial systems; (2) assessing, reporting, and tracking and monitoring correcting vulnerabilities identified during internal scans; and (3) ensuring all workstations are included in the scope of scans; and
- 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.

4. For Segregation of Duties:

   - Document incompatible duties that must remain segregated when granting and maintaining Traverse user access, and update existing policies and procedures to include requirements for properly segregating incompatible duties within Traverse.

5. For Contingency Planning:

   - Periodically test NEMIS backup tapes at a frequency that is in accordance with 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. If the NEMIS contingency plan cannot be tested, obtain DHS approved waiver, and implement effective compensating and mitigating controls; and
   - Update and appropriately test the TRRP and Traverse contingency plans and NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan, in accordance with DHS requirements for high impact systems, and test fail-over capability at the alternate processing site. Additionally, incorporate the Traverse and TRRP alternate processing facility and critical data files into the revised NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan.

After-Hours Physical Security Testing

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to media and equipment that housed financial data and information residing on a FEMA employee's / contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various FEMA locations that process and / or maintain financial data.

Conditions: Although not considered to be a material weakness, we noted the following other matters that resulted from our after-hours physical security testing during the FY 2009 audit engagement:

Exceptions Noted	Locations			Total Exceptions by Type
	FEMA Headquarters	Patriot's Plaza	FEMA Design Center	
Unprotected Passwords	18	19	5	**42**
External Memory Drives	0	2	2	**4**
For Official Use Only (FOUO)	0	1	1	**2**
Keys/Badges	0	0	2	**2**
Personally Identifiable Information (PII)	0	1	1	**2**
Server Names/IP Addresses	0	0	1	**1**
Unsecured Workstations or Laptops	0	1	0	**1**
Credit Cards	0	0	0	**0**
Classified Documents	0	0	0	**0**
Other –US government official passport	0	0	0	**0**
Total Exceptions by Location	**18**	**24**	**12**	**54**

Recommendations: We recommend that the appropriate FEMA management review the effectiveness of existing security awareness programs designed to protect electronic and physical data and ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical FEMA data and hardware. Additionally, FEMA employees and contractors should be made aware of the need to protect PII, as well as information marked "FOUO."

Causes/Effects for IT General Control Findings:

Many of these deficiencies originate from policy and system development activities that did not incorporate strong security controls from the outset and will take several years to fully remediate. While FEMA has made improvements in addressing the root cause of some IT deficiencies and has worked to improve security controls, we found that focus is often still placed on the tracking of responses to audit recommendations, instead of on developing the most effective method of addressing the actual control deficiency. When deficiencies in controls or processes are identified, we noted that corrective actions implemented address the symptom of the problem and do not always correct the root cause, resulting in a temporary fix. Further, detection of these temporary fixes through self-evaluation is not effective, due to insufficient testing of IT controls and remediation activities. Finally, FEMA has undertaken several high priority and competing IT initiatives to improve its control environment and does not always have sufficient resources to direct towards the implementation of security controls in a consistent manner.

Reasonable assurance should be provided that financial system user access levels are limited and monitored for appropriateness and that all user accounts belong to current employees and contractors. Furthermore, monitoring of the more highly privileged accounts is essential. The deficiencies identified in FEMA's access controls increase the risk that employees and contractors may have access to a system that is outside the realm of their job responsibilities or that a separated individual, or another person with knowledge of an active account of a terminated employee or contractor, could use the account to alter the data contained within the application or database without being detected. This may also increase the risk that the confidentiality, integrity, and availability of system controls and the financial data could be exploited, thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

The lack of fully implemented security configuration management controls may result in security responsibilities being improperly communicated to system developers as well as the improper implementation and monitoring of system changes. This also increases the risk of unsubstantiated changes and changes that may introduce errors or data integrity issues that are not easily traceable back to the changes. In addition, it increases the risk of undocumented and unauthorized changes to critical or sensitive information and systems, which may reduce the reliability of information produced by these systems.

The deficiencies in security management controls identified may result in systems being developed and implemented without proper identification and management of IT security risks. As a result, FEMA management decisions may be based on incomplete or inaccurate information, and IT controls may not be designed and implemented to adequately protect financial systems data and information. Additionally, the lack of implemented incident response procedures may result in suspected incidents not being appropriately detected, reported, and managed within the timeliness needed to prevent or minimize the impact to information resources. Finally, individuals who are unable to obtain favorable background investigations or who no longer have a need for access and privileges based on their employment status

and current job responsibilities, may be inappropriately granted and/or maintain access to financial systems and data.

A lack of segregation of duties policies and procedures may result in conflicting systems roles and privileges being granted to individuals. Additionally, if inappropriate data manipulation occurs, FEMA management may not be able to quickly determine if a segregation of duties conflict within roles and responsibilities resulted in the infraction and would have little recourse for taking action against users effectuating the violation.

The deficiencies related to contingency planning controls that we identified may result in FEMA's inability to recover financial systems and data during interruptions to financial processing so that operations can resume. Consequently, financial data may be lost or incorrectly processed. Moreover, deficiencies in contingency planning controls may negatively impact FEMA's national emergency management mission. Specifically, if FEMA were unable to recover and resume operations for NEMIS during states of emergencies or disasters, national response capabilities could be hindered.

Criteria for IT General Control Findings

The criteria used during our FY 2009 audit procedures over IT general controls consisted of Federal government and DHS IT security requirements. The *Federal Information Security Management Act* (FISMA), passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with Office of Management and Budget (OMB) and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines, including NIST Special Publication 800-53 (revision 2), *Recommended Security Controls for Federal Information Systems,* describe specific essential criteria for maintaining effective IT general controls. In addition, OMB Circular No. A-127, *Financial Management Systems*, prescribes policies and standards for Executive Branch departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. For this year's IT audit procedures, we also assessed FEMA's compliance with DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*.

APPLICATION CONTROL FINDINGS

We concluded that application controls over NEMIS, Core IFMIS, G&T IFMIS, and PARS could not be relied upon for purposes of our FY 2009 audit procedures because of the nature of 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, no application control weaknesses were identified during our FY 2009 testing at FEMA.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the FEMA management. The FEMA management agreed with all of our findings and recommendations. The FEMA management has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments in Appendix D.

OIG Response

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

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

Appendix A

Description of Key Federal Emergency Management Agency Financial Systems and Information Technology Infrastructure within the Scope of the FY 2009 Department of Homeland Security Integrated Audit Engagement

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

Below is a description of significant Federal Emergency Management Agency (FEMA) financial management systems and supporting information technology (IT) infrastructure included in the scope of the FY 2009 engagement to perform the financial statement audit.

Locations of Audit: FEMA Headquarters in Washington, D.C.; the Mount Weather Emergency Operations Center in Bluemont, Virginia; IT operations in Winchester, VA; the National Flood Insurance Program (NFIP) in Crystal City, Virginia; and the NFIP contractor location in Lanham, Maryland.

Key Systems Subject to Audit:

- *Core Integrated Financial Management Information System (IFMIS)*: Core IFMIS is the primary financial reporting system and has several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting).

- *Grants and Training (G&T) IFMIS*: G&T IFMIS was moved from the Department of Justice into the FEMA environment in FY 2007. The system stores former G&T financial information.

- *Payment and Reporting System (PARS):* PARS is a standalone web-based application that resides on the G&T IFMIS UNIX server. Through its web interface, PARS collects and stores Standard Form 269 information from grantees. Cron jobs are run daily to update the grant information from PARS into G&T IFMIS. Additionally, through these cron jobs, PARS is also updated with the obligation information from G&T IFMIS to provide updated information to its users.

- *National Emergency Management Information System (NEMIS)*: NEMIS is an integrated system to provide FEMA, states, and certain other federal agencies with automation to perform disaster related operations. NEMIS supports all phases of emergency management and provides financial related data to Core IFMIS via an automated interface.

- *Traverse*: Travers 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 Local Area Network Windows server in Lanham, MD. 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.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

Appendix B

FY 2009 Notices of Information Technology Findings and Recommendations at the Federal Emergency Management Agency

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

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

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

1 – Not substantial

2 – Less significant

3 – More significant

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

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

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-02	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-09-03	The process outlined for the Core Integrated Financial Management Information System (IFMIS) recertification that initiated on January 12, 2009, required that a new FEMA Form 20-24 be approved and submitted to the Financial Systems Section (FSS) for all current IFMIS users, and also required revocation of any accounts that could not be validated. However, we noted that the requirement to revoke access is not documented in the *Office of the Chief Financial Officer (OCFO) Procedures for Granting Access to IFMIS* or FEMA Instruction 2200.7, *IFMIS User Access Policy and Procedures*. We reviewed access authorization documentation for a selection of 40 active Core IFMIS user accounts, noted that 2 accounts did not have a FEMA Form 20-24 completed after January 12, 2009, and concluded that the accounts were not appropriately recertified and validated as belonging to current users. Additionally, access for the 2 accounts was not revoked, per the process described in the memorandum.	• Revise applicable FEMA policies and procedures to require that any accounts which are not positively verified during the periodic review of IFMIS accounts for recertification are revoked until a new approved FEMA Form 20-24 is received by FSS personnel. • Dedicate resources to ensure that consistent application of FEMA policies/procedures and DHS policy is performed by revoking access for all IFMIS application accounts not validated through submission of a new FEMA Form 20-24 as part of the periodic account review.	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-06	During the FY 2009 follow-up testwork, we noted that FEMA has obtained and distributed a reference guide that documents the purpose of Core IFMIS system security functions and their associated permissions and configuration options. However, the guide does not include policies and procedures addressing process requirements for adding, deleting, and modifying Core IFMIS system security functions. We also determined that no additional policies and procedures have been developed by FEMA or the IT developer of IFMIS that establish a process for implementing change controls for the maintenance of system security functions and their associated privileges. FEMA management represented to us that access to the security menu is limited, individuals with access to the menu do not use their privileges to delete, create, or modify functions, and changes are made to Core IFMIS system security functions through the standard change control process. However, we noted there are no controls in place to restrict and/or monitor the use of these privileges to ensure that system security functions are not modified, created, or deleted. Based on our testwork, we concluded that a formalized process for modifying specific Core IFMIS system security functions to ensure that appropriate privileges are created, documented, approved, and monitored does not exist.	Develop and implement policies and procedures documenting the process of adding, deleting, and modifying Core IFMIS system security functions to ensure that the proper controls are in place for modifying user account privileges. Additionally, these policies and procedures should include requirements over the monitoring of the usage of function modification privileges, configuration changes implemented for Core IFMIS system security functions, and requirements over updating system documentation for changes in the system security functions.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-12	The standard operating procedure (SOP) for recertification of National Emergency Management Information System (NEMIS) positions has not been finalized and implemented to require a semi-annual review of all user roles within the NEMIS Access Control System (NACS), including privileges related to access to specific NEMIS applications and modules. Furthermore, we determined that FEMA Enterprise Operations staff completed development of the technical infrastructure within NACS to support the recertification effort at the end of FY 2008. However, we determined that the FY 2008 recertification of NEMIS/NACS roles was not completed and FEMA initiated but did not complete the FY 2009 recertification that was scheduled for completion by April 30, 2009.	• Dedicate resources to complete the on-going review of NEMIS user access for FY 2009 and perform subsequent reviews, as required by DHS policy. • Finalize and fully implement formal procedures for conducting the NEMIS recertification process and retaining auditable records, in accordance with DHS policy. .	X		3
FEMA-IT-09-13	During FY 2009, we performed test work over security controls in place for Core IFMIS, NEMIS, and the FEMA iPass/virtual private network (VPN) remote access system, including follow-up testing on the prior year finding. Through comparison of active Core IFMIS, NEMIS, and iPass/VPN remote access accounts against a list of FEMA employees that had separated from employment since October 1, 2008, we determined that 1 Core IFMIS account, 62 NEMIS accounts, and 28 iPass/VPN accounts remained active and unlocked after the account holder's separation from FEMA. Additionally, of the 28 active iPass/VPN accounts, we determined that 11 also had at least one active NACS	• Evaluate and, if appropriate, revise existing procedures over removal of separated user access to IT systems to identify weaknesses that contribute to untimely removal of separated individuals from the information systems. • Ensure that procedures and processes are implemented consistently to remove system and application accounts for all separated users immediately upon notification of separation, in accordance with FEMA, DHS, and National Institute of Standards and Technology (NIST) guidance.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	role, indicating active remote access privileges to both the FEMA network and NEMIS.				
FEMA-IT-09-17	During the FY 2009 follow-up testwork, we noted that FEMA has a SOP that outlines the controls intended to address the risk associated with the Core IFMIS developers having the ability to migrate changes to the Core IFMIS production environment. The SOP, in particular, requires the locking and unlocking of the *ifmiscm* account during the implementation of software changes into production by system administrators. However, we determined that no formal procedures or processes are documented for performing reviews to verify that only authorized changes to the *ifmiscm* directory and sub-directories are implemented into production by the developers. Additionally, we determined that although informal reviews of the directories were performed during the fiscal year, they were not routinely completed, and documented evidence of the reviews performed was not retained.	Implement compensating controls to address the risk associated with the segregation of duties weakness related to developers making changes to the production environment. Specifically, FEMA should develop and implement policies and procedures for conducting periodic reviews to verify that only authorized changes are made to the Core IFMIS production directories and subdirectories by developers using the *ifmiscm* account. Additionally, the policies and procedures should include requirements for retention of auditable evidence of the reviews that are performed.	X		2
FEMA-IT-09-19	FEMA Enterprise Operations personnel informed us that the SOP, *Monitoring Sensitive Access to NEMIS,* was developed to outline the process for monitoring sensitive access to the NEMIS operating system. Based upon our review of the SOP, we noted that a list of NEMIS servers that are considered to be within the scope of the SOP are listed, but that specific hosts and server designations are not clearly defined. In particular, approximately 30 separate IT components are described, and certain servers supporting web-	• Revise the SOP, *Monitoring Sensitive Access to NEMIS*, to ensure that it states that the scope of the procedures includes all servers defined in up-to-date system documentation as supporting NEMIS system software within system boundaries for the financial applications and modules. • Acquire and deploy appropriate tools on system software and operating systems	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	facing applications for registration, applicant inquiry, and assistance processing are listed. However, based on additional testwork and corroborative inquiry of NEMIS personnel, we determined that at least 170 operating system servers for NEMIS are not comprehensively included in the scope of the SOP. Additionally, FEMA informed us that outlined procedures for conducting the required reviews of audit trails every 3 days and retaining evidence for at least a year have not been implemented and the NEMIS operating system activity is not currently being logged or monitored. Additionally, we noted that no application or tool is currently in place to support the audit logging function on the NEMIS Linux server. Consequently, we concluded that FEMA has partially addressed the prior year recommendation by including review and retention requirements in the SOP for monitoring NEMIS activity. However, the SOP has not been implemented on the operating system software supporting NEMIS and does not include all NEMIS operating system servers within its scope.	supporting the NEMIS financial applications 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.			
FEMA-IT-09-22	During our FY2009 follow-up testwork, we noted that FEMA was unable to take corrective action to establish and implement an alternate processing site for the NEMIS application. Additionally, a current waiver over the lack of an alternate processing site did not exist. FEMA security personnel described compensating controls surrounding the contingency planning	• 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 a waiver for approval in accordance with DHS policy	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	process. Specifically, FEMA management informed us that in FY 2009 the NEMIS Contingency Plan was partially tested through an annual table-top exercise to restore five of the NEMIS servers from backup tapes at the Mt. Weather Emergency Operations Center (MWEOC). Furthermore, FEMA management informed us that compensating controls were also provided through performance of full backups of critical NEMIS data on a regular basis and the transfer of these tapes to an offsite backup storage facility. However, during further testwork and analysis, we determined that there were weaknesses in the compensating controls described by FEMA management. In particular, we noted that while the contingency plan was tested, a full restore of all the of the NEMIS servers was not performed. Additionally, backup tapes for NEMIS are not fully tested on a periodic basis. (Please refer to NFRs FEMA-IT-09-24 and FEMA-IT-09-25 for further information.)	regarding waivers, and ensure that compensating controls over the alternate processing site are effective and documentation of their effectiveness is maintained as auditable records.			
FEMA-IT-09-24	In FY 2009, we conducted follow-up procedures to determine if FEMA had implemented corrective action for the prior year finding and determined that NEMIS backup tapes were not regularly tested during FY 2009.	Periodically test NEMIS backup tapes at a frequency that is in compliance with FEMA and DHS policy.	X		2
FEMA-IT-09-25	During our FY 2009 audit, we conducted follow-up procedures and determined that full-scale testing of the NEMIS Contingency Plan, in accordance with DHS requirements for high impact availability systems, has not been conducted. FEMA provided us with the testing results of limited table-top testing that	• Update the NEMIS Contingency Plan so that it meets the requirements of DHS policy for high impact availability systems. Additionally, ensure that the plan comprehensively addresses the numerous sub-systems within NEMIS so that detailed	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	was performed to test the local restoration for 4 of approximately 170 servers that comprise NEMIS. However, the DHS-approved waiver obtained in FY 2008 that listed table-top testing as a compensating control for FEMA's inability to fully test NEMIS was expired. In FY 2009, we also determined that the existing NEMIS 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 names and information over the various modules of NEMIS, was not appropriately documented to reflect the current operating environment. • The contingency plan did not include detailed procedures necessary to fully restore the NEMIS application in the event of an emergency. • System/Application Recovery Priority Classification have not been defined. • Service Level Agreements and Memorandum of Understandings (MOU) were not included in the plan. • The Business Impact Analysis included in the contingency plan was completed in 2004 and was not adequately documented.	information exists over the current system architecture, critical processing priorities, detailed SOPs for systems recovery and other required components in accordance with DHS guidance. • Conduct documented annual tests of the NEMIS Contingency Plan that address all critical phases of the plan, and update the plan with lessons learned, as necessary and in accordance with DHS and NIST requirements. • If the NEMIS contingency plan cannot be tested in accordance with DHS guidance for high impact availability systems, develop, implement, and document effective compensating and mitigating controls.			
FEMA-IT-09-28	In FY 2009, we performed follow-up testwork over NEMIS non-emergency system changes that occurred	In accordance with DHS and FEMA policy, ensure that when implementing the new NEMIS	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	under the process established during the time frame of October 1, 2008 to February 28, 2009 prior to the change in the NEMIS development contractors. Specifically, of the 25 NEMIS non-emergency application level System Change Requests (SCR) tested, we noted the following exceptions: • 7 of 25 SCRs did not obtain documented SCR approval prior to development; • 21 of 25 SCRs did not obtain documented Technical Development Laboratory (TDL) approval prior to implementation in the test environment; • 2 of 25 SCRs did not obtain documented Technical Review Committee (TRC) approval prior to implementation into production; and • 8 of 25 SCRs did not have testing documentation to demonstrate that testing occurred.	non-emergency change control process that all required approvals are obtained prior to development and implementation of changes into production. Additionally, ensure that the appropriate testing is conducted and that the testing documentation is appropriately retained according to FEMA and DHS policy.			
FEMA-IT-09-29	We tested a selection of 3 NEMIS emergency application level SCRs that occurred in the time frame of October 1, 2008 to February 28, 2009 before NEMIS configuration management responsibility was transitioned to the new contractor. Of the 3 SCRs tested, we noted that 1 was missing the required initial approval prior to moving the change into the TDL environment for testing.	In accordance with DHS and FEMA policy, ensure that when implementing the new NEMIS emergency change management process that all required approvals are obtained prior to development and implementation of changes into production. Additionally, ensure that the appropriate testing is conducted and that the testing documentation is appropriately retained according to FEMA and DHS policy.			3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-38	In FY 2009, we performed follow-up test work and determined that the National Flood Insurance Program (NFIP) contractor had documented system roles and had implemented capabilities for enforcing segregation of duties for users within the Traverse application currently. Also, as a mitigating control, the NFIP contractor reviews a User Log report generated by Traverse for each financial user's system access, which is reviewed and signed off on every month to ensure that the appropriate privileges are assigned. However, incompatible duties that must remain segregated when granting and maintaining user access to the Traverse application have not been documented. We were also reviewed the *Traverse Standard Operating Procedure (SOP) for Financial Processes* and noted that it states that a Traverse user log is produced to show appropriate user access to perform accounting duties and usage of the Traverse accounting system. However, the SOP does not include policies and procedures regarding segregating incompatible duties within Traverse.	Continuing with our prior year recommendation, document Traverse duties that are incompatible, and develop and implement policies and procedures for properly segregating incompatible duties within the system when granting and maintaining access.	X		1
FEMA-IT-09-39	The Traverse and Transaction Reporting and Recording Processing (TRRP) Contingency Plan has not been tested, and a test of the system fail-over capability at the alternate processing site has not been conducted. Also, we did not receive the requested NFIP Certification & Accreditation (C&A) package that includes the Traverse and TRRP Contingency Plan and the test results. As a result, we determined that a current contingency plan for the TRRP and	• Complete the documentation and testing of the TRRP and Traverse Contingency Plan, to include all critical phases of the plan in accordance with DHS policy requirements for high impact systems. In addition, conduct a test of the system fail-over capability at the alternate processing site, and ensure that TRRP and Traverse processing is tested in	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Traverse applications does not exist. At the time of our audit testwork, we were informed that due to delays in implementation of the new system of record, NFIP and the NFIP IT contractor had initiated efforts FEMA's Chief Information Security Officer (CISO) to recertify and accredit the NFIP legacy system and update and test the Traverse and TRRP Contingency Plan and NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan. Furthermore, the NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan provided for auditor review does not incorporate the Traverse and TRRP alternate processing facility or TRRP critical data files.	accordance with DHS guidance. • Revise the NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan to incorporate the Traverse and TRRP alternate processing facility and the TRRP critical data files in accordance with DHS guidance for high impact systems. Additionally, the revised plan should be tested and updated with lessons learned from the testing.			
FEMA-IT-09-45	We determined that access for Core IFMIS Oracle database users was appropriately documented and authorized. Thus, this portion of the prior year recommendation, as it relates to the Core IFMIS database, is closed. Additionally, we reviewed a selection of 40 Core IFMIS Forms 20-24 (access request forms) for users who were either new IFMIS users during the fiscal year or whose access profile changed during the fiscal year outside of the recertification process. We determined that of the 40 active application users tested: • Two users did not have a completed Form 20-24 on file;	• Review and revise the Office of the Chief Financial Officer's existing *Procedures for Granting Access to IFMIS* to require authorization of new and modified Core IFMIS user accounts by supervisors, program managers, and contracting officers' technical representatives (COTRs) in accordance with DHS guidance. The requirements should also include the retention of Core IFMIS access authorization documentation. • Develop and implement of policies and procedures over periodic recertification of all user access to the Core IFMIS Oracle database, and retain auditable records in	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• FEMA was unable to provide evidence that the initial account creation of 10 accounts during FY 2009 was authorized; and • FEMA was unable to provide evidence that modifications to account privileges for 10 accounts were authorized. FEMA management additionally informed us that recertification of IFMIS Oracle database accounts had not been performed during FY 2009. Consequently, we concluded that while certain corrective actions to address weaknesses over Core IFMIS account management have been implemented, FEMA has not consistently maintained documentation for initial account creation or subsequent account modification for the application, and FEMA has not developed or implemented a process to recertify accounts on the IFMIS Oracle database.	accordance with DHS policies and procedures as evidence that recertifications are conducted and completed periodically. Additionally, if the Core IFMIS/Grants and Training (G&T) IFMIS merger is performed in FY 2010, ensure that a recertification of IFMIS Oracle accounts is performed prior to the merger.			
FEMA-IT-09-46	We determined that a MOU and Interconnection Sharing Agreement (ISA) was documented, accepted, and signed by FEMA and the Department of the Treasury on April 22, 2009. Consequently, while the prior-year recommendation was addressed, the interconnection was operating without authority for a majority of the fiscal year, and the NFR is re-issued.	No recommendation is required for this weakness that existed for the majority of FY 2009 because it was remedied on April 22, 2009 when the MOU and ISA were signed by FEMA and Department of the Treasury management.		X	1

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-48	During the FY 2009 audit, we were informed that internal vulnerability scans are conducted every month on the NEMIS systems. However, FEMA personnel informed us that identified vulnerabilities and related corrective actions are reported and tracked via emails and not documented in Plan of Action and Milestones (POA&M).	Complete planned corrective actions to develop and implement an SOP that outlines the process for formally reporting and tracking resolution of weaknesses identified during internal NEMIS vulnerability scans in accordance with DHS guidance.		X	3
FEMA-IT-09-50	During FY 2009 follow-up testwork, we obtained evidence that "superuser" activity reports for Core IFMIS were appropriately reviewed by FSS personnel in accordance with FEMA and DHS policy. Consequently, this portion of our recommendation for prior year NFR FEMA-IT-08-50 is closed. However, FSS personnel informed us that failed database login attempts and activity performed by application users with the "superuser" role remain the only forms of activity logged and monitored for Core IFMIS. Other activity on the application and database required to be logged by DHS policy, including successful logins, access modifications, and changes to user profile, are not enabled within Core IFMIS. Additionally, we noted that a procedure does not exist to establish the process for reviewing and retaining evidence of these logs once the configurations are implemented. FEMA reported in the FY 2008 audit remediation plan that internal instructions describing the review process for these two reports were documented. We reviewed the SOP, *Monitoring of IFMIS Database Audit Logs*, and determined it addresses the process for reviewing	• Revise and implement policies and procedures that document requirements for configuring, retaining, and reviewing audit trails for the Core IFMIS application and database, in accordance with DHS policy. Additionally, ensure that all DHS requirements are met through this process, including appropriate supervisory review and retention. • Implement configurations on the Core IFMIS application and database in accordance with DHS policy to ensure that audit logs sufficiently record required auditable events and activities.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	the daily Oracle failed login report. However, documented instructions concerning the review of weekly "superuser" reports were not provided to us during the audit.				

FEMA-IT-09-51	During our FY 2009 integrated test work, IT Enterprise Operations personnel informed us that the *SOP for Handling of Oracle Audit Logs* was implemented for the databases specified in the SOP and that evidence of audit log reviews are retained. However, we noted that weaknesses in NEMIS database audit controls still exist, as follows:
	• During our inspection of the SOP, we noted that it requires the procedures to be performed for two specific NEMIS databases, the National Processing Service Center (NPSC) database and the Consolidated Master database. However, through additional testwork, we noted that NEMIS has at least 23 databases. Consequently, not all of the databases that comprise NEMIS are included within the scope of the SOP, and we were informed by IT Enterprise Operations personnel that no additional SOPs exist that address auditing logging for the remaining 21 databases.
	• The SOP has not been updated to require that successful logins, access modifications, highly privileged user account activity, and changes to user profiles are logged and reviewed.
	• On four of the NEMIS databases related to financial processing that we selected for testing,
		• Revise and enforce the *SOP for Handling of Oracle Audit Logs* to ensure that the procedures are developed and implemented in accordance with DHS guidance, to include:
		  • All databases within the defined system boundaries that support NEMIS financial applications and modules within the scope of the SOP,
		  • Requirements for audit logging and retention of audit trails,
		  • Periodic reviews of audit trails for NEMIS databases, and
		  • Appropriate segregation of duties principles.
		• Implement configurations on NEMIS databases in accordance with DHS policy over required auditable events and activities.
			X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	we determined that configurations are not fully enabled so that a review of audit trails and activity defined by DHS policy requirements can be completed. • Based on our review of audit log documentation, we noted that reviews of audit logs for NEMIS databases are performed by the database administrators (DBAs) who have been assigned administrator privileges to administer the databases. Thus, we determined that database audit log review duties are not appropriately segregated from DBA duties.				
FEMA-IT-09-52	In FY 2009, we performed follow-up testwork and were informed that FEMA is currently in the process of updating the NEMIS patch management policy and that the finalized policy had not been implemented. However, FEMA could not provide us with a copy of the requested draft policy that was reported as under development for our review. Based on additional inquiry, we also determined that the timeframe for implementing patches on FEMA systems has not been established, in accordance with DHS guidance.	Dedicate the appropriate resources to complete efforts to document, finalize, and implement comprehensive patch management policies and procedures for NEMIS, in accordance with DHS policy. Additionally, ensure that these procedures include requirements for responding to DHS Security Operations Center (SOC) and DHS Computer Security Incident Response Center (CSIRC) notifications to ensure compliance with the timely implementation of required patches.			3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-53	During our FY 2009 audit, we reviewed FEMA's Remediation Plan, and we noted that FEMA management had reported that corrective action to update the *NEMIS SSP* had been fully implemented. We obtained the *NEMIS SSP* dated February 16, 2009 for our review and noted that the plan had been revised since our prior year audit. However, upon further inspection, we determined that the current plan does not fully document the system's boundaries, define all of the NEMIS subsystems and major applications, nor establish security responsibilities for the various system components.	Ensure that *NEMIS SSP* is updated in accordance with DHS policy so that the system's boundaries, components, and responsibilities surrounding the various subsystems and major applications of NEMIS are accurately and comprehensively documented in the plan.		X	2
FEMA-IT-09-54	In FY 2009, we performed testwork over Traverse configuration management. Upon inspection of the *System Change Control Procedures,* that address Traverse configuration management, we noted that the procedures outline steps for controlling changes during the change control process for Traverse. However, the procedures do not include comprehensive configuration management guidance that addresses the following elements required by FEMA and DHS policy: • configuration identification • configuration control • version control • configuration status accounting • configuration audits • establishment of a Change Control Board (CCB) or TRC for evaluating changes prior to	Ensure the implementation of an updated version of the current Traverse configuration management procedures that comprehensively addresses FEMA and DHS requirements.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	production.				
FEMA-IT-09-56	Based on observations conducted with FSS and G&T IFMIS database personnel, we identified the following weaknesses in database security controls: • A manual review of inactive G&T IFMIS database accounts is performed on a monthly basis to disable accounts which have not been used in the past 90 days. However, since IFMIS is categorized as a high impact system, reviews are required to identify accounts that have been inactive for 45 days. • Strong passwords are not required and/or enforced for G&T IFMIS database accounts. • Emergency and temporary access to the G&T IFMIS database, including access for contractor development personnel, is approved by the FSS Chief and/or their staff, not by the FEMA CISO/Information System Security Manager (ISSM) or a designee, as required by DHS policy.	• Revise the formal process for reviewing and disabling inactive G&T IFMIS Oracle database user accounts to adhere to DHS policy over disabling inactive accounts on high impact systems. • Configure all G&T IFMIS Oracle database user accounts to adhere to DHS policy for passwords and authenticator controls. • Establish a formal process for granting emergency and temporary IFMIS G&T database access that includes segregation of duties considerations and appropriate approval from FEMA management in accordance with DHS policy.	X		3
FEMA-IT-09-57	Based on observations conducted with FSS and G&T IFMIS database personnel, we determined that Oracle database audit trails are not configured to capture any activity, including failed login attempts or administrator-level actions.	• Configure the G&T IFMIS databases to log events and retain audit records in accordance with DHS policy; and • Develop and implement policies and procedures surrounding the requirements for G&T IFMIS database audit logging to include the periodic review of database audit logs in accordance with DHS policy.			3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-58	Based on corroborative inquiry with FSS and application and database administrators, we concluded that a management review to validate the appropriateness of G&T application and Oracle database user accounts has not been formally implemented or performed by FSS this fiscal year. Additionally, FSS management further informed us that no recertification of accounts was conducted when the application was acquired and brought online at FEMA in FY 2007 and has not been conducted since.	• Establish a formalized process for the recertification of the G&T IFMIS application and database accounts or include G&T IFMIS in the scope of the formalized processes for the recertification of Core IFMIS application and database accounts. Additionally, ensure that the established processes are developed and implemented in accordance with DHS guidance. • Conduct an immediate recertification of user account access on the G&T IFMIS application and Oracle database to validate the continued appropriateness of access as being commensurate with job responsibilities.	X		3
FEMA-IT-09-59	In FY 2009, we performed test work over the G&T "ifmiscm" account to determine the controls in place for the migration of changes into production. The "ifmiscm" account is 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 are also responsible for migrating application code changes into the production environment using the "ifmiscm" account. Additionally, when we inspected the account, the G&T "ifmiscm" account was not locked on May 15, 2009, which allowed the contractor unrestricted access to the production environment. We were further informed by FEMA personnel that access to that	• Limit the contracted developers' access to the G&T IFMIS production environment to "read only," and segregate the responsibility for deploying application code changes into production from the contractor to an independent control group. • If business need requires that the segregation of duties cannot be immediately implemented, document policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	account is not limited or monitored on a periodic basis.				
FEMA-IT-09-60	During our testwork, we concluded that the "Legacy NFIP IT System" C&A pertaining to the Traverse application, TRRP application, and NFIP Local Area Network (LAN) expired on October 4, 2008. Consequently, the legacy system has since been operating without a current Authorization to Operate (ATO). Furthermore, we were not provided the requested NFIP C&A package consisting of the following artifacts: • Federal Information Processing Standard (FIPS) 199 Categorization • Privacy Impact Assessment • E-Authentication • Risk Assessment • SSP • Contingency Plan • Security Test and Evaluation • Contingency Plan Testing • Security Assessment Report • ATO • Annual NIST SP 800-53-based Self-Assessments	Immediately work with FEMA's CISO to complete the recertification and accreditation of the NFIP legacy system in accordance with applicable DHS policies and Federal guidance.	X		2
FEMA-IT-09-61	The G&T instance of IFMIS was brought online at FEMA in FY 2007 after acquisition from the Department of Justice. However, we determined that a C&A of the system had not been performed, and the	• Formally designate an ISSO and DAA for G&T IFMIS. • Immediately work with FEMA's Information	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	system has not received an ATO. Specifically, the following C&A elements have not been completed, documented, or approved for G&T IFMIS and will not be for the remainder of the fiscal year: • FIPS 199 categorization • Privacy Impact Assessment • E-Authentication • Risk Assessment • SSP • Contingency Plan • Security Test and Evaluation • Contingency Plan Testing • Security Assessment Report • ATO • Annual NIST SP 800-53-based Self-Assessments In addition, we determined that at the time of our test procedures, neither an ISSO nor a Designated Authorizing Authority (DAA) had been formally designated for the G&T instance of IFMIS by FEMA management.	Security Office to certify and accredit the G&T IFMIS instance in accordance with applicable DHS policies and Federal guidance. If FEMA management makes a business decision to conduct a C&A of IFMIS after the merger and not over the existing G&T IFMIS instance, as a mitigating control, immediately conduct an assessment of key controls to identify security weaknesses and determine the operational risks related to IFMIS G&T. The weaknesses identified should be documented with plans for accelerated remediation efforts or related risks should be formally accepted by FEMA in accordance with DHS guidance.			
FEMA-IT-09-62	We reviewed the *VPN Rules of Behavior for Users Behind Corporate Firewalls*, dated December 5, 2002, and noted that individual VPN access request forms are required to be completed, approved by managers, and submitted to the National Help Desk, Enterprise Service Desk (ESD). However, we noted that the requirements do not include approval by the system owner or a designated representative, as required by	• Revise and implement policies and procedures for documenting, reviewing, and approving individual VPN user accounts for employees of external entities requiring access to the FEMA network via VPN access, and ensure that sufficient resources are dedicated to appropriately authorize accounts on behalf of the system owner or a designee, according to	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	DHS policy. We reviewed a blank VPN Access Request Form and noted that an approval block titled "For FEMA Office of Cyber Security (OCS) Use Only" is included and that the form states that all VPN requests must be approved by the FEMA OCS. We reviewed a selection of 25 completed forms for active VPN user accounts and determined that, while the forms were approved by the requestor's manager or supervisor, none of the forms had an approval noted by OCS or an appropriate designated representative of the system owner. Additionally, we were informed by FEMA IT security personnel that OCS, as referred to in the Rules of Behavior and the request form, 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. Additionally, we were informed that 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. VPN accounts are managed within the FEMA LAN, specifically the Active Directory environment, and subsequently added to the Cisco Access Control Server (ACS) that permits VPN access. However, through test work conducted over the FEMA LAN, we determined that a recertification of network user accounts is not performed.	FEMA and DHS policy. • Develop and implement policies and procedures in accordance with DHS policy to perform a periodic recertification of all VPN user access and retain auditable records as evidence that recertifications are conducted and completed periodically.			

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-63	We noted the following weaknesses in the process for authorizing remote VPN access to external organizations, including state emergency management agencies and FEMA contractors: • 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 individuals using non-DHS equipment to access the FEMA network. Additionally, we noted that the current process in place for granting remote access to the FEMA network through VPN is not in compliance with FEMA, DHS, and NIST guidance. Specifically, we noted the following weaknesses: • 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.	• 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, FEMA should 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 Component CISO/ISSM to connect to non-DHS equipment. • Draft and formalize ISAs, MOUs, and MOAs delineating security responsibilities by FEMA and external organizations when connecting through non-DHS equipment to the FEMA network via VPN access. 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. • Ensure that agreements related to VPN access are reviewed and recertified on a periodic basis, specifically, when a major system change occurs or every three years, in	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Two-factor authentication is not used for VPN access, as required by DHS policy. • 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 the Inter-Agency VPN Agreements have not been documented and that this requirement is inconsistent with DHS policy, which requires 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 site surveys were outdated, did not contain the level of technical granularity describing the external network security controls required to appropriately approve a connection to the FEMA LAN, and were not independently verified for accuracy by FEMA. Additionally, we determined that DHS guidance indicates that a single ISA may be used for multiple connections	accordance with DHS policy. • Implement and require two-factor authentication for all remote access to the FEMA network, including VPN and all other tools used for remote access, in accordance with DHS policy and FIPS 140-2.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	provided that the security accreditation is the same for all connections covered by that ISA. However, we determined that the security accreditation of multiple connecting networks listed in single ISAs with external entities is not being evaluated by the FEMA SOC to ensure the security requirements are appropriately implemented.				
FEMA-IT-09-64	The Core IFMIS database is not configured to retain a history of account passwords in order to prevent reuse. However, DHS guidance requires passwords to be configured so that users cannot reuse the last eight passwords.	• Configure the Core IFMIS Oracle database to enforce DHS policy requirements regarding the reuse of user passwords. • Develop and implement procedures to ensure that those with systems administration and security responsibilities over the Core IFMIS database environment are made aware of DHS, FEMA and Federal system security requirements and guidance and are properly trained in those requirements and guidance.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-65	We determined that of 40 access request forms (Form 20-24) for active G&T IFMIS application users selected: • FEMA was unable to provide documented evidence that the initial account creation of 11 accounts in FY2009 were authorized; and • FEMA was unable to provide documented evidence that modifications to account privileges for 11 accounts were authorized. Additionally, we requested for review a selection of eight G&T IFMIS Oracle Database User Access Control Forms for G&T IFMIS Oracle database users whose accounts were created during the fiscal year. We determined that of the eight users selected, two did not have documented evidence that the accounts were authorized or appropriately approved prior to creation.	Review and revise the Office of the Chief Financial Officer's existing *Procedures for Granting Access to IFMIS* to specifically require the authorization of new and modified G&T IFMIS user accounts by supervisors, program managers, and/or contracting officers' technical representatives for the G&T IFMIS application and database in accordance with DHS guidance. The requirements should also include retention guidance for G&T IFMIS access authorization documentation.	X		3
FEMA-IT-09-66	Based on observations conducted with IT Enterprise Operations database personnel over the four databases selected for test work that process NEMIS financial data, we determined that DBA account passwords are not required to be "strong passwords." Specifically: • No minimum password length is enforced. • Password complexity is not required so that passwords include a combination of upper/lowercase letters, numbers, and special characters. • Reuse of previous passwords is not prohibited. • Passwords are not configured to expire and forced to be changed after a predetermined length of	• Configure all NEMIS Oracle databases to enforce the DHS policy for passwords and authenticator control requirements, including expiration, reuse, and length and complexity. • Develop and implement procedures to ensure that those with systems administration and security responsibilities over the NEMIS database environment are made aware of DHS, FEMA and Federal requirements and guidance and are properly trained in those requirements and guidance.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	time.				
FEMA-IT-09-67	Based on observations conducted over the FEMA domain policy and an end-user workstation, we determined that workstations are configured to activate a password-protected screensaver after 15 minutes of inactivity, rather than the five minute inactivity threshold required by DHS policy.	Implement the plan to 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.	X		2
FEMA-IT-09-68	We determined that a C&A of the Payment and Reporting System (PARS) was not performed and the system had not received an ATO. Specifically, no evidence exists to support that the required C&A elements have been completed, documented, or approved for PARS. In addition, we determined that at the time of our test procedures, neither an ISSO nor a DAA had been formally designated by FEMA management for PARS.	• Formally designate an ISSO and DAA for PARS. • Immediately work with FEMA's Chief Information Security Office to certify and accredit PARS in accordance with applicable DHS policies and Federal guidance.	X		3
FEMA-IT-09-69	Upon inspection of the *NFIP Technical Services Department Production Systems Control Unit Procedures,* that addresses TRRP configuration management, we noted that the procedures outline steps for controlling changes during the change control process for TRRP. However, the procedures do not include a comprehensive configuration management guidance that addresses the required elements for a comprehensive configuration management plan in accordance with FEMA and DHS policy. Furthermore, we performed testwork over initial	Ensure implementation of an updated version of the current TRRP configuration management procedures that comprehensively addresses FEMA and DHS requirements. The updated procedures should require initial approvals of OSRs and establish a process for obtaining CCB and TRC approvals prior to implementing changes into production, in accordance with DHS policies and procedures.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	approval, testing, and implementation of a selection of 25 TRRP changes made in FY 2009 and noted the following exceptions: • 16 out of the 25 changes did not obtain initial Operating System Request (OSR) approvals prior to developing the change. • All 25 changes did not obtain TRC or CCB approval for production implementation.				
FEMA-IT-09-70	We were informed by the NFIP contractors that no patch management policy and procedures exist for the Windows operating system which supports the Traverse application and the NFIP LAN. Additionally, we determined that while NFIP has documented the *Traverse System Software Procedures* which outline the process to initiate, approve, test, and implement operating system upgrades into production, the procedures do not specifically address patch management. Furthermore, the procedures do not provide robust guidance for approving, installing, and testing patches, according to DHS requirements.	Document, finalize, and implement comprehensive patch management policies and procedures for the NFIP LAN and the Traverse operating system, in accordance with DHS policy. Additionally, ensure that this procedure includes requirements for authorizing, testing, and approving patches to be implemented into production and responding to DHS SOC and DHS CSIRC notifications to ensure compliance with the timely implementation of required patches.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-71	During our after-hours physical testing, we identified 42 written unprotected passwords, 4 external memory drives, 2 documents labeled as 'For Official Use Only (FOUO)', 2 badges, 2 instances of unsecured Personally Identifiable Information (PII), 1 instance of a written server name with an Internet Protocol (IP) address, and 1 unsecured laptop.	Review the effectiveness of existing security awareness programs designed to protect electronic and physical data, and ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical FEMA data and hardware. Additionally, FEMA employees and contractors should be made aware of the need to protect PII, as well as information marked "FOUO."	X		2
FEMA-IT-09-72	Through discussions with FSS personnel, we determined that the description of mitigating and compensating controls noted in the approved DHS Waivers and Exceptions Request for Core IFMIS does not accurately reflect the operating environment for the Core IFMIS application and database. Specifically: • Successful database connections are not logged, as described. • Superuser activity is monitored at the application level. However, no other audit logs or records described in the request are reviewed. • The exception request states that "direct access to the IFMIS database is restricted to approximately 70 users, and is read-only in nature for the purposes of running ClearAccess report functions;" however, direct access to the database includes DBAs with read/write privileges in addition to ClearAccess read-only users. • Approval was granted by the DHS CISO with an added condition that FEMA periodically capture	• Submit a revised DHS Waivers and Exceptions Request Form that accurately reflects the mitigating and compensating controls in place on the Core IFMIS environment to justify exception from DHS policy concerning audit logging on the Core IFMIS database. • Ensure that future waiver and exception requests involve the input, review, and approval of system owners and administrators to provide adequate assurance that the documented risk mitigation strategies accurately reflect security controls in place. • Ensure that FEMA establishes a more formal communication process for providing approved waivers back to system owners so that any requirements for the implementation of additional controls are reviewed and executed appropriately and timely.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	the audit records at a database level and compare them to the application logs to ensure that data is correct at the application level. However, the requirement had not been implemented at the time of our FY 2009 audit procedures. Consequently, we concluded that the request for an exception to DHS policy requirements related to audit logging for the Core IFMIS Oracle database was approved by the DHS CISO based on inconsistent or inaccurate information about the system environment and current controls in place to mitigate the risk of not implementing DHS policy. Additionally, the DHS CISO's condition for granting approval has not been met by FEMA.				

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-73	Based on observations conducted with FEMA IT security personnel and IFMIS UNIX system administrators, we determined that the "root" account access 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 local access to the root account is not locked down. Additionally, FEMA has not enforced the use of the switch user command, "sudo," which requires system administrators to login with their userID and switch over to the root account to ensure who is accessing the account is logged and authorized. Additionally, we determined that 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.	• Develop and implement policies and procedures over the monitoring of system administrator and highly-privileged account activity in the Core and G&T IFMIS UNIX environments, in accordance with FEMA and DHS policy. • Implement technical controls to restrict access to the "root" account through the use of "sudo" to ensure that explicitly authorized individuals only have access to the account. • Ensure that system logs and records of administrator activity, including "sudo" activity related to the "root" account, are retained and reviewed by IT security management independent of the system administration team.	X		3
FEMA-IT-09-74	FEMA's systems inventory does not include all financial systems. Specifically, G&T IFMIS and PARS were not included in the inventory provided to us during the audit by FEMA, and neither system is being tracked via the Trusted Agent Federal Information Security Management Act.	Update the FEMA system inventory to include the G&T instance of IFMIS, as well as PARS. Comply with DHS policy and consistently follow procedures for updating and monitoring the FISMA system inventory to ensure that all new and current systems are accounted for with complete and accurate information, in accordance with NIST and DHS policy.	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-75	During the audit, we determined that review of access to the NFIP data center is performed on an ad-hoc basis. However, there are no policies or procedures that require periodic and documented recertification of data center access at a defined frequency.	Document defined and repeatable procedures for the review of physical access to the NFIP data center in accordance with DHS and NIST guidance. These procedures should, at a minimum, define the frequency of this review and what documentation should be maintained as evidence of that review.	X		1
FEMA-IT-09-76	Based on testwork performed and inquiries conducted with FSS and Core IFMIS database personnel, we determined that emergency and temporary access to the database, including access for contractor development personnel, is approved by the FSS Chief and/or their staff, rather than by the FEMA CISO/ISSM or a designee, as required by DHS policy. Additionally, we determined that the Core IFMIS Oracle database access granted to contracted development personnel to implement database changes to Core IFMIS conflicts with segregation of duties principles.	Establish a formal process for granting emergency and temporary Core IFMIS database access that includes segregation of duties considerations and appropriate approval from FEMA management in accordance with DHS policy.	X		3
FEMA-IT-09-77	FEMA 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 Office of the Chief Information Officer (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.	Define and implement formal and repeatable processes to ensure that financial systems development and acquisition projects are conducted in compliance with DHS systems engineering life cycle (SELC) and acquisition requirements as well as Federal guidance. The processes should 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	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		involvement of all stakeholders and relevant FEMA management, establishment of Acquisition Decision Events at each SELC phase, and integration of IT security considerations throughout all project phases.			
FEMA-IT-09-78	Based on our testwork, we concluded that NEMIS configuration management is not adequately 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 new development contract have not been documented and approved by FEMA management, in accordance with DHS and FEMA policy. • Once the new systems development contractor delivers developed changes to FEMA, FEMA does not monitor and track NEMIS SCRs throughout the configuration management lifecycle, from initial approval through implementation into the production environment. Instead, FEMA only tracks and collects documentation for SCRs from Project Managers at the final approval stage when the request is	• Document and implement a comprehensive configuration management plan for NEMIS which clearly defines the roles and responsibilities for FEMA and contractor personnel managing the development of non-emergency and emergency system changes, in compliance with DHS and FEMA requirements. • Ensure that NEMIS non-emergency and emergency system changes are tracked, controlled, properly documented, and managed by FEMA personnel throughout the lifecycle of the configuration management process in accordance with DHS and FEMA guidance and policies.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	received by the TRC.				
FEMA-IT-09-79	Based on observations conducted over the FEMA LAN and the Microsoft Windows Active Directory (AD) environment, we concluded that the following weaknesses exist: • The FEMA LAN domain security policy does not enforce password requirements in accordance with DHS policy. • Policies and procedures over the authorization of FEMA LAN accounts, independent of NACS approval process outlined in the *Non-User Specific, Shared, Other Group Type Accounts SOP*, have not been finalized or implemented. Additionally, we determined that initial access authorizations for a selection of AD accounts were not authorized. • A periodic recertification of FEMA LAN access accounts is not currently performed to ensure that access is still necessary and appropriate for each individual. • We compared a listing of active FEMA LAN/AD accounts against a list of FEMA employee separations that had occurred since October 1, 2008. Based on our test work, we determined that 36 accounts remained active and unlocked after the account holder's separation from FEMA.	• Revise the FEMA LAN and AD account policies to require strong passwords, in accordance with DHS policy. • Finalize and fully implement the *Non-User Specific, Shared, Other Group Type Accounts SOP*. Specifically, FEMA should ensure that policies and procedures over the granting and managing of access for group/shared/service and administrator-level user accounts not authorized through NACS are documented and implemented consistently. Additionally, policies and procedures should ensure that, in accordance with DHS policy, a clear business need is established and documented justifying the creation and use of these types of accounts. • Develop and implement a formal process for performing a periodic recertification of user access to the FEMA LAN which defines requirements and addresses users not accounted for during the planned recertification of NEMIS application access. • Evaluate and, if appropriate, revise existing procedures over removal of separated user access to ensure that all separated users on the FEMA LAN are removed in a timely manner.	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		Ensure that procedures and processes are implemented consistently to remove network accounts for all separated users immediately upon notification of separation, in accordance with FEMA, DHS, and NIST guidance.			
FEMA-IT-09-80	NFIP has not developed and implemented formal procedures that outline the process for conducting internal scans for the NFIP LAN and for assessing, reporting, and correcting identified weaknesses. We also determined that remediation of vulnerabilities identified during internal scans of the NFIP LAN is not formally tracked and monitored through the POA&M Process in accordance with DHS policy. While the NFIP contractor conducts internal vulnerability scans of the NFIP LAN on a monthly basis, scanning of select workstations are presently excluded.	• Develop and implement formal procedures that outline the internal scan processes and requirements. These procedures should include, at a minimum, the process for assessing, reporting, and correcting weaknesses identified during scans. Additionally, ensure that the scope of vulnerability scans conducted include all workstations on the NFIP LAN. • With the involvement of both FEMA management and NFIP contractors, implement procedures for formally tracking and monitoring the remediation of vulnerabilities identified during the internal scans of the NFIP LAN through FEMA's POA&M process.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-81	FEMA does not have approved and finalized procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of Core and G&T IFMIS. FEMA also provided us with documented evidence of a G&T IFMIS internal vulnerability scan that was performed on July 17, 2009. However, we noted that the scan was scheduled and performed after our initial request for audit documentation. Additionally, FEMA was unable to provide us with any evidence that prior scans of G&T IFMIS had been performed or scheduled since the system was brought online in FY 2007.	• Establish and formalize FEMA policies and procedures over the requirements, processes, and responsibilities for performing periodic vulnerability scans for Core and G&T IFMIS instances, in accordance with DHS guidance. • Ensure that vulnerability assessment scans are performed for G&T IFMIS and that weaknesses identified are formally reported and tracked for remediation through the DHS POA&M process, as required by DHS guidance.	X		2
FEMA-IT-09-82	Upon inspection of the FEMA SOP for installing UNIX patches to the Core and G&T IFMIS instances, we noted that it does not outline the process for defining a timeline for implementing non-emergency and emergency patches or for authorizing, testing, and approving patches for implementation, in accordance with DHS guidance. Furthermore, FEMA IT personnel informed us that documented test results of UNIX patches are not retained by IT personnel after testing is completed.	Document, finalize, and implement comprehensive patch management policies and procedures for Core and G&T IFMIS, in accordance with DHS policy. Policies and procedures should include requirements for responding to DHS SOC and DHS CSIRC notifications to ensure the timely implementation of required patches and retention of testing documentation.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-83	We were informed by FEMA IT System Integrations that NEMIS' program directories for the TDL environment, where all User Acceptance Testing (UAT) occurs, and the NEMIS production environment where the code changes are implemented, are located on one server. Upon review of the processes for restricting access to these directories, we noted the following weakness: • Of the fifteen individuals with access to the server, 3 accounts belonged to development personnel who have write, read, execute, and modify access to all of the server's directories, which allow unrestricted access to both the production and development environments for NEMIS. • FEMA does not lock down the code in its server directory environment, giving all accounts unrestricted access to the NEMIS TDL and production environment after the code has been approved for implementation. 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 of not locking down the directories.	• Develop and implement a formalized a process and procedures for restricting and monitoring access over the NEMIS production 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 the monitoring of NEMIS system directories to ensure that no changes have occurred after the approval of NEMIS system changes has occurred. • Limit the developers' access to the NEMIS production directories to "read only" and segregate the responsibility for delivering application code changes into the NEMIS directory server from the contractor to an independent control group. If business need requires that the segregation of duties cannot be immediately implemented, document policies and procedures to compensate for the risk associated with the segregation of duties weakness noted, in accordance with DHS guidance.	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-84	Based on testwork performed, we identified the following weaknesses in PARS database security controls: • PARS database accounts are not reviewed to identify accounts that have been inactive for 45 days or more, as required by DHS policy for high impact systems. • Strong passwords are not required and/or enforced in accordance with DHS requirements. • Database audit logs are not configured to capture auditable events, including failed login attempts and administrator-level actions. • A periodic recertification of PARS database access accounts is not currently performed to ensure that access is still necessary and appropriate for each individual. FEMA could not provide evidence that initial PARS database granted to one of four users was appropriately authorized and the individual was inappropriately approved for emergency database access by the FSS Chief, rather than the FEMACISO/ISSO/ISSM or designee, as required by DHS policy.	• Perform documented periodic reviews of PARS database accounts and disable inactive accounts, in accordance with DHS policy. • Configure PARS database accounts to adhere to DHS policy for passwords and authenticator controls, including expiration, reuse, and complexity. • Configure the PARS databases to log events and conduct documented reviews of audit logs, in accordance with FEMA and DHS policy. • Further define and implement a formal process that documents requirements for configuring, retaining, and reviewing audit trails for the PARS database in accordance with FEMA and DHS policy. Additionally, ensure that all DHS requirements are met through this process, including appropriate supervisory review and retention. • 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.	X		3

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-85	Based on observations conducted with the NFIP IT contractor, we determined that while TRRP system passwords were configured to enforce password complexity using alphabetic, numeric, and special characters, the configurations did not limit the use of dictionary words. Additionally, the password configuration did not prevent the password from being any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, in accordance with DHS guidance.	No recommendation is required for this weakness that existed for the majority of FY 2009 because it was remedied prior to the end of the audit when the TRRP password settings were reconfigured to enforce complexity requirements that exceed DHS requirements.	X		2
FEMA-IT-09-86	We noted that the 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. Additionally, we determined that NFIP does not have a formal process for monitoring changes that the vendor makes in Traverse while logged in as an administrator.	• In accordance with policy, establish a separate account for the third-party vendor's use to implement Traverse changes, and limit use of the account so that it is activated on an as needed basis. • Establish and implement a formal process for monitoring and verifying configuration changes made by the vendor in the Traverse environment, in accordance with DHS policy. Additionally, ensure that these procedures include requirements for documentation retention.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-87	Procedures for management of FEMA IT security incidents have not been developed, approved, and implemented, in accordance with FEMA and DHS requirements. Additionally, our unannounced FY 2009 vulnerability assessment scanning activity was not detected and appropriately reported by FEMA IT personnel in accordance with DHS and FEMA policy.	• Develop, approve, and implement an SOP for managing security incidents that clearly outlines roles and responsibilities required to maintain a continuous incident response capability, as required by DHS and FEMA policy. • Provide training to all personnel with incident response roles and responsibilities.	X		2
FEMA-IT-09-88	During our FY 2009 audit testwork, we noted that NFIP had not formally established a process for authorizing, documenting the approval and business need for service accounts, and recertifying service accounts on the TRRP system. As a result, authorization forms were not on file for all service accounts, and recertifications of access are only conducted for user accounts.	• Revise the TRRP access control policies and procedures to ensure that the creation of service accounts are appropriately authorized and that a clear business need is established and documented justifying the creation and use of these types of account in accordance with DHS policy. • Ensure that policies and procedures over TRRP access authorization include a formalized process for the recertification of service accounts on an annual basis in accordance with DHS policy.	X		2
FEMA-IT-09-89	FEMA did not adequately conducted suitability investigations for FEMA federal employees in accordance with DHS requirements, and position designations associated with employees with elevated system privileges did not have appropriate position sensitivity designations. We also determined that formal procedures were not developed or implemented for conducting suitability screenings of contractors accessing DHS IT systems.	• Further define and refine processes to ensure that background investigations for all types of federal employees are performed in accordance with DHS directives. • Reevaluate and assign the correct position sensitivity levels to federal employees with access to DHS information systems in accordance with DHS policy.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Additionally, suitability investigations were not appropriately conducted for contractors with access to multiple FEMA information systems holding sensitive IT security positions, and the contractors did not have position sensitivity designations.	• 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 contracting personnel in accordance with DHS policy. • Ensure that all systems owners formally and correctly define the appropriate suitability designation for contracting personnel needing access to their information systems in accordance with DHS policy. Additionally, ensure that position sensitivity designations distinguish between various levels of access and require the contractor to have their suitability investigation completed prior to being granted access.			
FEMA-IT-09-90	We determined that FEMA has certified the FEMA Switch Network (FSN)-2 switch network, which is comprised of various FEMA LANs across the regions and each LAN is classified as a subsystem of the switch network. During our review of the C&A package, we noted that the Maryland (MD) National Processing Service Center (NPSC) is considered to be a subsystem to the overarching General Support System (GSS) FSN-2 and that the primary servers for NEMIS, Core IFMIS, and G&T IFMIS financial applications reside on this portion of the LAN. However, the document states that no current accreditation or certification letters could be found for	• Formally designate an ISSO and DAA for the MD NPSC. • Immediately conduct an assessment of key controls that help ensure confidentiality and availability of data for security weaknesses, and determine the operational risk related to MD NPSC LAN supporting FEMA financial applications. Weaknesses identified should be documented with plans for accelerated remediation efforts, or related risks should be formally accepted by FEMA. • Review and revise the FSN-2 C&A package	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	that subsystem during the certification and accreditation of the FSN-2 package. Specifically, there is no evidence in the package that the required C&A elements have been completed/updated, documented, or approved for MD NPSC in accordance with DHS guidance. We further noted that the C&A package states that C&A activities are to be completed for the MD NPSC subsystem at a separate time and that no security roles were defined for the MD NPSC within the C&A. We inquired with FEMA Information Technology (IT) Security and management to determine the status for the MD NPSC C&A package and were not provided with any additional information as to the status of the C&A package. Additionally, upon further review of the C&A package, we noted that both the MD NPSC and the regional LANs are within scope of this review as NEMIS has servers at multiple regional sites. Furthermore, we determined that management had not adequately completed the C&A package over FSN-2 according to DHS policy.	to reflect the current GSS environment in accordance with DHS and Federal guidance. Additionally, ensure that the C&A Package has been completed to include the required artifacts, addresses the security controls for the various subsystems, and assigns and updates the appropriate security roles for each subsystem.			
FEMA-IT-09-91	FEMA does not have a formal process for adequately tracking FEMA contractors throughout the on-boarding, termination, and transfer processes. Furthermore, we noted that the process established for notifying the FEMA OCIO 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.	Document and implement procedures, according to DHS guidelines and requirements, that track the on-boarding, transfer, and separation of contractors. Ensure that the policies and procedures include: • The assignment of roles and responsibilities to appropriate FEMA management and stakeholders.	X		2

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Specifically, there are no formal requirements for COTRs to notify the OCIO of separating contractors.	• Steps for notifying the FEMA OCIO that a contractor is separating or transferring so that the contractor will have their systems access removed or modified in a timely manner, in accordance with DHS policies. • Regularly distribute a listing of terminated contract personnel to information system administrators so they can remove user access timely.			

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

Appendix C

Status of Prior Year Notices of Findings and Recommendations (NFR) and Comparison to Current Year NFRs at the Federal Emergency Management Agency

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-08-02	During our vulnerability assessment technical testing, certain configuration management weaknesses were identified on Integrated Financial Management Information System (IFMIS) and National Emergency Management Information System (NEMIS) database instances and on key support servers. Specifically, servers were identified with password and auditing configuration weaknesses		FEMA-IT-09-02
FEMA-IT-08-03	IFMIS accounts did not complete a new Federal Emergency Management Agency (FEMA) Form 20-24 in response to the recertification process.		FEMA-IT-09-03
FEMA-IT-08-06	We noted that FEMA has made a management decision not to develop policies and procedures over the modification of IFMIS account functions until the new IFMIS system upgrade occurs. We noted that FEMA has reported in the Plan of Action and Milestones (POA&M) that they expect to address corrective action for this weakness in FY 2010. As a result, a formalized process does not exist to guide Financial Services Section (FSS) staff in the modification of the system to ensure that appropriate privileges are created, documented, and approved for a specific function.		FEMA-IT-09-06
FEMA-IT-08-12	FEMA informed us that the automated manager certification process has not yet begun. Therefore, the FY 2008 recertification has not been completed and the risk of unauthorized users accessing NEMIS was present for a majority of the fiscal year.		FEMA-IT-09-12
FEMA-IT-08-13	We were informed that terminated IFMIS users are to have the "DELETEUSER" role applied to their account profile prior to being removed from the application, which overrides all existing roles and deactivates any existing privileges within the application although the individual can still log into the account. However, FEMA Instruction 2200.7 specifies that personnel separating from FEMA shall have all IFMIS access privileges cancelled and their user account removed. Consequently, although the risk is mitigated by the limited access rights on the accounts with the "DELETEUSER" privilege, those six accounts demonstrate that the policies and procedures surrounding the IFMIS terminated user process are not consistently applied and the accounts have not been removed. Additionally, 4 out of the 10 accounts remained on the IFMIS system with an active status.		FEMA-IT-09-13

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-08-17	There is no documented evidence to support that monitoring of the "ifmiscm" directory and sub-directories is occurring.		FEMA-IT-09-17
FEMA-IT-08-19	While FEMA informed us that system software activity is logged, we were unable to obtain evidence that the audit logs were reviewed on a periodic basis.		FEMA-IT-09-19
FEMA-IT-08-22	Per inspection of the POA&M, we noted that corrective action was initiated by FEMA to implement an alternate processing facility for NEMIS, but that the alternate site has not been established. Due to the magnitude of the project scope, implementation of an alternate processing site will not be achieved within 12 months. Consistent with DHS policy for corrective actions that cannot be implemented within 12 months, a Department of Homeland Security (DHS) Information Technology (IT) Security Program Waiver (number WR-2008-012) was approved by the DHS Chief Information Security Officer (CISO) in March 2008 to provide FEMA with additional time to plan and develop an effective alternate processing site for NEMIS. Per DHS policy, the waiver must be reviewed, updated, and re-approved by the appropriate management officials every six months. As required by DHS policy, the approved waiver describes the mitigating efforts, management's acceptance of the associated residual risk, and a plan for attaining compliance with DHS policy. The waiver also documents the compensating controls to mitigate risk until the alternate processing site is implemented. The compensating controls are to be derived by conducting annual table-top exercises and ensuring that regular backups of critical NEMIS data and offsite backup storage are performed. However, a fully successful table-top test of NEMIS has not been conducted for FY 2008. The waiver granted provides an extension of time to implement corrective action, but the associated risk still remains.		FEMA-IT-09-22
FEMA-IT-08-23	IFMIS system administrators conducted ad hoc backup tape restores for system users and performed a full database restore in March 2008 during a server upgrade. However, there was no evidence that quarterly testing was conducted or that FEMA has a formalized process to test backup tapes more frequently than annually.	X	

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA IT-08-24	We noted that the tape restore schedule requires quarterly testing of backup tapes beginning no earlier than FY 2009. Additionally, we determined that the NEMIS contingency plan was not tested and consequently a full NEMIS backup tape restore did not occur in FY 2008. Rather, NEMIS system administrators conducted ad hoc backup tape restores at the request of system users during the fiscal year.		FEMA-IT-09-24
FEMA-IT-08-25	Due to the magnitude of the project scope to establish a "real-time" alternate processing site for NEMIS, FEMA was unable to implement corrective actions to fully remediate the prior year finding within 12 months. Consistent with DHS policy for findings that cannot be remediated within 12 months, a DHS IT Security Program Waiver (number WR-2008-012) was approved by the DHS CISO in March 2008 to provide FEMA with additional time to plan and develop an effective alternate processing site for NEMIS. Per DHS policy, the waiver must be reviewed, updated, and re-approved by the appropriate management officials every six months. The waiver identifies that until the alternate processing site is implemented and full scale testing can be conducted, compensating controls will be implemented by conducting annual table-top exercises. Additionally, at the close of our audit test work, we determined that annual table-top testing had not been conducted and documented. We determined that the most recently conducted table-top review of NEMIS contingency plan occurred on July 21, 2007 and was conducted for processes, procedures, and scenarios identified in the contingency plan dated June 29, 2007. We noted that the documented results of the July 2007 test stated that FEMA was unable to successfully complete steps that were planned to be conducted during the Recovery Procedure Activation phase due to material weaknesses and deficiencies cited in the recovery procedures.		FEMA-IT-09-25

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-08-28	During our FY 2008 follow up test work, we tested a selection of 40 NEMIS non-emergency application level Software Change Requests (SCR) that had occurred since October 1, 2007. Of the 40 SCRs tested, we noted the following exceptions: • 29 SCRs did not have testing documentation attached to the SCR; • 36 SCRs did not obtain Test and Development Laboratory (TDL) approval; and • 32 SCRs did not obtain Technical Review Committee (TRC) approval.		FEMA-IT-09-28
FEMA-IT-08-29	We noted that TRC approvals for NEMIS application level emergency changes did not consistently follow FEMA and DHS guidance. Specifically, we determined that of 25 emergency NEMIS changes selected for testing: • 22 changes did not have documented TRC approval; • 4 did not gain SCR approval prior to implementation into production; • 16 did not gain TDL approval; and • 6 did not have related testing documentation attached.		FEMA-IT-09-29
FEMA-IT-08-38	We were referred to Section 2.2.1 of the *National Flood Insurance Program (NFIP) Local Area Network (LAN) Administrative Manual* as guidance on segregating incompatible duties. Based on our review of the manual, we noted that it does not include policies and procedures regarding segregating incompatible duties within Traverse. Additionally, while we noted that system roles and responsibilities have been documented, Traverse duties are incompatible are not documented.		FEMA-IT-09-38
FEMA-IT-08-39	During our test work, we noted that a planned update and subsequent testing of the Traverse Contingency Plan was not conducted and that system fail over capability at the alternate processing site had not been tested. Additionally, the NFIP Disaster Recovery and Continuity of Operations Plan was not updated to include the Transaction Recording and Reporting Processing (TRRP) and Traverse alternate processing facility or TRRP critical data files and restoration priorities.		FEMA-IT-09-39
FEMA-IT-08-45	IFMIS user access is not managed in accordance with account management procedures.		FEMA-IT-09-45

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
FEMA-IT-08-46	The existing Memorandum of Understanding with the Department of Treasury expired in October 2007.		FEMA-IT-09-46
FEMA-IT-08-47	Based upon our review, we determined that the Interconnection Sharing Agreement between FEMA and the Small Business Administration expired in July 2007 and has not been reauthorized and reissued, as required by DHS policy.	X	
FEMA-IT-08-48	The vulnerabilities identified from the NEMIS scans are not reported and tracked via DHS' POA&M process.		FEMA-IT-09-48
FEMA-IT-08-49	We noted that the software was improperly configured so that the user's ability to change the following settings had not been disabled: • File System Auto-Protect for automatically scanning system files for threats, known viruses, and worms on a continuous basis when Windows is started; • Microsoft Exchange Auto-Protect for automatically scanning Outlook and/or Outlook Express messages for viruses. • Lotus Notes Auto-Protect for automatically scanning incoming and outgoing Lotus Notes messages; and • Internet Email Auto-Protect for scanning all incoming and outgoing e-mail messages other than Outlook and/or Outlook Express.	X	
FEMA-IT-08-50	We performed test work over audit logging on the IFMIS application and Oracle database. Based upon inquiry and inspection of documentation, we determined that on a daily basis, an automated report is generated and emailed to the database administrators and FSS personnel for review. However, while this report is distributed for review by the database administrators and FSS staff, no evidence that the reviews are conducted is retained. Additionally, we noted that while FEMA Instruction 2200.7, *IFMIS User Access Instruction*, assigns the responsibility of conducting this weekly review to FSS, FEMA personnel do not formally document that the review is conducted.		FEMA-IT-09-50
FEMA-IT-08-51	We noted that the Standard Operating Procedure (SOP) does not comprehensively address requirements of FEMA Directive 140-1, *FEMA IT Security Policy*. Specifically, the SOP does not require the monitoring of modifications to account tables and other highly-privileged and administrator-		FEMA-IT-09-51

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
	level activities. Additionally, we noted that the SOP requires database administrators to initial and retain printed logs as evidence that reviews are conducted as required. However, FEMA informed us that this portion of the SOP was not being performed.		
FEMA-IT-08-52	Finalization and implementation of the *Security Operations Center SOP - FEMA Information Security Vulnerability Management*, which specifies the timeframe for installing security patches, has been delayed due to organizational changes.		FEMA-IT-09-52
FEMA-IT-08-53	Upon inspection of the NEMIS System Security Plan (SSP) that is a part of the certification and accreditation (C&A) package; we noted that the server and host names listed in Appendix B of the SSP are not accurate. Specifically, the listing of system components is not comprehensive and portions of information, such as system owners, are not up to date.		FEMA-IT-09-53
FEMA-IT-08-54	In FY 2008, we determined that NFIP had documented and implemented the *Traverse System Change Control Procedures*. During the audit, we determined that two Traverse changes had been implemented since October 1, 2007. We obtained change documentation for both changes and noted that testing documentation was not retained for these changes.		FEMA-IT-09-54
FEMA-IT-08-55	During our FY 2008 test work, we noted that NFIP documented and implemented the *NFIP Technical Services Department Production Systems Control Unit Procedures* that provide guidance on implementing changes into the production environment. We selected for testing eight TRRP changes that had been implemented since October 1, 2007. Of the eight tested, we identified that test results were not available for one change.	X	

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

FEMA

APR 21 2010

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 FEMA FY 2009 Financial Statement Audit*, dated March 2010

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.

FEMA concurs with each of 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. The Governance and Investment Integration Branch (GIIB), the CIO created the GIIB to manage audit activities, will hold weekly meetings with Action Officers to review the status of implementing these recommendations and address issues that are impeding progress. Branch Chiefs will receive weekly reports reflecting the current status of their organization's assigned actions and will work diligently to correct findings and implement recommendations.

FEMA develops and maintains a detailed Plan of Action and Milestones (POA&M) for each audit recommendation in the DHS Trusted Agent FISMA (TAF) system. We believe these POA&Ms provide the specific responses to each audit recommendation that you requested. 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 Landon V. Cochran, Chief, Governance and Investment Integration Branch, at 202-646-8272.

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2009

Report Distribution

Department of Homeland Security

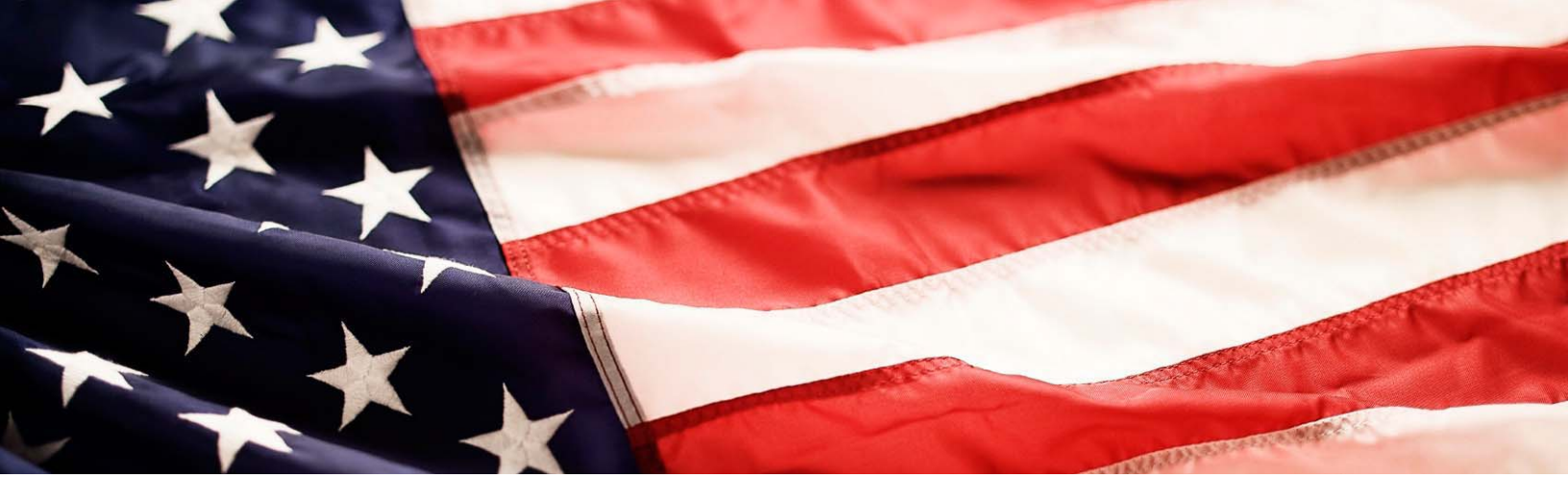
Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Administrator, FEMA
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, FEMA
Chief Information Officer, FEMA
Chief Information Security Officer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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or 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.