Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2008 DHS Financial Statement Audit

(Redacted)

Notice: The Department of Homeland Security, Office of Inspector General has redacted the report for public release. A review under the Freedom of Information Act will be conducted upon request.

OIG-09-48

March 2009

Office of Inspector General

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

Homeland
Security

March 27, 2009

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 2008 DHS financial statement audit as of September 30, 2008. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-09-09, November 2008) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of DHS' FY 2008 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 5, 2008, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or make 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 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 5, 2008

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 consolidated balance sheet of the U.S. Department of Homeland Security (DHS) as of September 30, 2008, and the related statement of custodial activity for the year then ended (referred to herein as "financial statements"). We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources for the year ended September 30, 2008 (referred to herein as "other financial statements"). Due to matters discussed in our Independent Auditors' Report, dated November 14, 2008, 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 connection with our fiscal year (FY) 2008 engagement, we considered 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 in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982* (FMFIA). The objective of our engagement was not to provide an opinion on the effectiveness of DHS' internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of DHS' internal control over financial reporting. Further, other matters involving internal control over financial reporting 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, 2008, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other FY 2008 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects DHS' ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of DHS' financial statements that is more than inconsequential will not be prevented or detected by DHS' internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

During our audit engagement, we noted certain matters 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 general and application controls. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 14, 2008. This letter represents the separate restricted distribution report mentioned in that report.

Although not considered to be material weaknesses, we also noted certain other matters during our audit engagement which we would like to bring to your attention. These matters are also described in the *IT General Control 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 **For Official Use Only**. We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. In addition, we have provided: a description of key FEMA financial systems and IT infrastructure within the scope of the FY 2008 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated December 5, 2008.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General, OMB, 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, 2008

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008

OBJECTIVE, SCOPE AND APPROACH

We were engaged to perform audit procedures over Department of Homeland Security (DHS) information technology (IT) general controls in support of the fiscal year (FY) 2008 DHS balance sheet and statement of custodial activity audit engagement. The overall objective of our engagement was to evaluate the effectiveness of 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. The scope of the IT general controls assessment performed at the Federal Emergency Management Agency (FEMA) 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 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 six control functions to be essential to the effective operation of the IT general controls environment.

- *Entity-wide security program planning and management (EWS)* – 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.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software controls (SS)* – Controls that limit and monitor access to powerful programs that operate computer hardware and secure applications supported by the system.
- *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.
- *Service continuity (SC)* – 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, as well as testing over key financial application controls. The technical security testing was performed both over the Internet and from within select FEMA facilities, and focused on test, development, and production devices that directly support FEMA's financial processing and key general support systems.

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 (APC)* - 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 2008, FEMA took corrective action to address prior year IT control weaknesses. For example, FEMA made improvements by restricting access to offline account tables, implementing an alternate processing site for one of its financial applications, and improving the process for retaining National Flood Insurance Program (NFIP) change control documentation. However, during FY 2008, we continued to identify IT general control weaknesses at FEMA. The most significant weaknesses from a financial statement audit perspective related to controls over access to programs and data and controls over program changes. 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 weaknesses negatively impacted the internal controls over FEMA 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). The applicable IT findings were combined into one material weakness regarding IT in our *Independent Auditors' Report*, dated November 14, 2008, on the DHS consolidated financial statements.

Of the 26 findings identified during our FY 2008 testing, 15 were repeat findings, either partially or in whole from the prior year, and 11 were new findings. These findings were representative of five of the six key FISCAM control areas, and the majority were inherited from the lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS 4300A, *Information Technology Security Program,* requirements and National Institute of Standards and Technology (NIST) guidance. Specifically, the findings stem from: 1) inadequately designed and operating access control policies and procedures relating to the granting of access to systems and supervisor re-certifications of user access privileges, 2) lack of properly monitored audit logs, 3) inadequately designed and operating change control policies and procedures, 4) patch and configuration management weaknesses within the system, and 5) the lack of tested contingency plans. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and FEMA financial data could be exploited, thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

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

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

Conditions: In FY 2008, the following IT and financial system control weaknesses were identified at FEMA and contribute to a DHS-level significant deficiency that is considered a material weakness in IT general and application controls:

1. Access controls – we noted:
   - User account lists were not periodically reviewed for appropriateness, resulting in inappropriate authorizations and excessive user access privileges;
   - Accounts were not disabled or removed promptly upon personnel termination;
   - Audit logs were not reviewed or evidence of audit log reviews was not retained; and
   - Security patch management and configuration weaknesses exist on hosts supporting the key financial applications and general support systems.

2. Application software development and change controls – we noted:
   - Emergency and non-emergency changes were made prior to management approval. Additionally, changes made to the system did not always follow established procedures. Specifically, [redacted], test plans, test results, approvals, and software modifications were not consistently performed or documented.

3. System software – we noted:
   - Evidence of system software audit log reviews is not retained.

4. Service continuity – we noted:
   - An alternate processing site is not operational for one of the FEMA financial systems.

5. Entity-wide security program planning and management – we noted:
   - Vulnerabilities identified from periodic scans are not reported and tracked via the Plan of Action and Milestones (POA&M) process.

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

1. For access controls:
   - Develop and appropriately implement an access authorization process that ensures that a request is completed and documented for each individual prior to granting him/her access to a financial application or database;
   - Implement an account management certification process within FEMA to ensure the periodic review of user accounts for appropriate access and ensure that current user profiles are appropriately documented;
   - Implement a process to ensure that all system accounts of terminated employees and contractors are immediately removed/end-dated/disabled upon their departure;
   - Develop and implement detailed procedures requiring the consistent and timely review of operating system and application logs for suspicious activity and the maintenance of documentation supporting such reviews; and
   - Conduct periodic vulnerability assessments, whereby systems are periodically reviewed for access controls related to patch management and configuration management not in compliance with DHS and other Federal guidance, and ensure that corrective action is developed, tracked, and performed to remediate any security weaknesses identified.

2. For application software development and change control:
   - Further develop and enforce policies that require changes and emergency changes to the application software to be approved, tested, and documented prior to implementation, and related documentation to be appropriately maintained.

3. For system software:
   - Actively monitor the use of and changes related to operating systems and other sensitive utility software and hardware, and maintain evidence of this monitoring.

4. For service continuity:
   - Ensure that alternate processing sites are established and made operational.

5. For entity-wide security program planning and management:
   - Ensure that all vulnerabilities and weaknesses are reported and tracked via the POA&M process.

Other Findings in IT General Controls

Although not considered to be a material weakness, we also noted the following other matters related to IT and financial system control deficiencies during the FY 2008 audit engagement:

1. Access controls – we noted:
   - Interconnection Security Agreements (ISA) between FEMA and external parties were not in place or not finalized;
   - A formalized process does not exist to guide staff in the modification of system accounts to ensure that appropriate privileges are created, documented, and approved for a specific function;
   - Instances of inadequate or weak passwords that existed on key systems, servers and databases that house financial data; and
   - Workstations were configured without up-to-date anti-virus software.

2. Service continuity – we noted:
   - Full testing of a current and finalized contingency plan was not conducted; and
   - Backup tapes are not tested on a quarterly basis.

3. System software – we noted:
   - Procedures for identifying and installing patches are in draft and have not been implemented; and
   - Developer changes to the directory and sub-directories of one financial application are not monitored to review and validate implemented changes.

4. Entity-wide security program planning and management – we noted:
   - The system security plan for one financial system is not accurate and up-to-date.

5. Segregation of duties – we noted:
   - Documentation surrounding incompatible roles and responsibilities does not exist over a key financial application, and policies and procedures for properly segregating incompatible duties within the system are not documented.

Recommendations: We recommend that the FEMA OCIO and FEMA OCFO, in coordination with the DHS OCIO and OCFO, make the following improvements to FEMA's financial management systems:

1. For access controls:
   - Ensure that ISAs are documented and finalized between FEMA and all applicable external parties;
   - Develop and implement policies and procedures that document the process of adding, deleting, and modifying [redacted] functions to ensure that the proper controls are in place for modifying user account privileges;
   - Enforce password controls that meet DHS' password requirements on all key financial systems; and
   - Develop procedures to regularly review and monitor workstations to ensure that the most up-to-date virus protection software is installed.

2. For service continuity:
   - Perform testing of key service continuity capabilities, including contingency planning. Ensure that all contingency plans and related documentation are updated upon completion of testing; and
   - Test backup tapes at least quarterly.

3. For system software:
   - Implement a patch management policy and enforce the requirement that systems are periodically tested for vulnerabilities by FEMA and the DHS OCIO; and
   - Establish a process within existing procedures for retaining documented evidence that developer changes to a financial application directory and sub-directories are monitored to verify that only authorized changes are implemented into production.

4. For entity-wide security program planning and management:
   - Finalize and implement the comprehensive system security plans for all key financial systems in accordance with DHS and NIST guidance.

5. For segregation of duties:
   - Document duties that are incompatible, and develop and implement policies and procedures for properly segregating incompatible duties within the system.

Cause/Effect: Many of these weaknesses 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 weaknesses 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 weakness. When weaknesses 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 weaknesses identified within 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.

Furthermore, the lack of fully implemented security configuration management controls may result in security responsibilities communicated to system developers improperly 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.

Criteria: 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 OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines 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

No application control weaknesses were identified during our FY 2008 testing of IT controls.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from FEMA Management. Generally, FEMA agreed with all of our findings and recommendations. FEMA has developed a remediation plan to address these findings and recommendations. We have incorporated these comments where appropriate and included a copy of the comments at Appendix D.

OIG Response

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

Appendix A

Description of Key Federal Emergency Management Agency Financial Systems and Information Technology Infrastructure within the Scope of the FY 2008 Department of Homeland Security Financial Statement Audit Engagement

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008

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 engagement to perform the financial statement audit.

Locations of Audit: FEMA [redacted].; the [redacted] in [redacted]; the National Flood Insurance Program (NFIP) in [redacted]; and the NFIP contractor location in [redacted].

Key Systems Subject to Audit:

- [redacted] – [redacted] is the key financial reporting system, and has several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting).

- [redacted] – [redacted] is an integrated system to provide FEMA, the states, and certain other federal agencies with automation to perform disaster related operations. [redacted] supports all phases of emergency management and provides financial-related data to [redacted] via an automated interface.

- [redacted] ([redacted] - The [redacted] application acts as a central repository of all data submitted by the Write Your Own (WYO) companies and [redacted] Direct Servicing Agent. [redacted] also supports the NFIP, primarily by ensuring the quality of financial data submitted by the WYO companies and the Direct Servicing Agent to [redacted]. [redacted] is a [redacted]-based application that runs on the NFIP [redacted] logical partition in [redacted]

- [redacted] - The general ledger application used by [redacted] to generate the NFIP financial statements. [redacted] is a client-server application that runs on a [redacted] server in [redacted], which is secured in the [redacted] room. The [redacted] client is installed on the desktop computers of the [redacted] Bureau of Financial Statistical Control group members.

- [redacted] - [redacted] is a web-based application which was developed by [redacted] specifically for FEMA grants. [redacted] allows grantees to access their grant funds and upload SF 269s online. Draw down transaction information from [redacted] is interfaced with [redacted]. [redacted] then interfaces with the U.S. Department of the Treasury (Treasury) to transfer payment information to Treasury, resulting in a disbursement of funds to the grantee.

Appendix B

FY 2008 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, 2008

Notice of Findings and Recommendations – Definition of Risk Ratings:**

The Notices of Findings and Recommendations (NFR) were risk ranked as High, Medium, and Low** based upon the potential impact that each weakness could have on Federal Emergency Management Agency's (FEMA) information technology (IT) general control environment and the integrity of the financial data residing on FEMA's financial systems, and the pervasiveness of the weakness.

** **The risk ratings are intended only to assist management in prioritizing corrective actions**, considering the potential benefit of the corrective action to strengthen the IT general control environment and/or the integrity of the DHS consolidated financial statements. The risk ratings, used in this context, are not defined by *Government Auditing Standards*, issued by the Comptroller General of the United States, or the American Institute of Certified Public Accountants (AICPA) Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Professional Standards and reported in our *Independent Auditors' Report* on the DHS consolidated financial statements, dated November 14, 2008.

Correction of some higher risk findings may help mitigate the severity of lower risk findings, and possibly function as a compensating control. In addition, analysis was conducted collectively on all NFRs to assess connections between individual NFRs, which when joined together could lead to a control weakness occurring with more likelihood and/or higher impact potential.

High Risk**: A control weakness that is more serious in nature affecting a broader range of financial IT systems, or having a more significant impact on the IT general control environment and /or the integrity of the financial statements as a whole.

Medium Risk**: A control weakness that is less severe in nature, but in conjunction with other IT general control weaknesses identified, may have a significant impact on the IT general control environment and / or the integrity of the financial statements as a whole.

Low Risk**: A control weakness minimal in impact to the IT general control environment and / or the integrity of the financial statements.

Federal Emergency Management Agency
FY 2008 Notices of Information Technology
Notices of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
FEMA-IT-08-02	During our vulnerability assessment technical testing, certain configuration management weaknesses were identified on [redacted] and [redacted] database instances and on key support servers. Specifically, servers were identified with password and auditing configuration weaknesses.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		**X**	**High**
FEMA-IT-08-03	[redacted] account users did not complete a new FEMA Form 20-24 in response to the recertification process.	Ensure that the Office of Chief Financial Officer (OCFO) Procedures for Granting Access to [redacted] are consistently followed by continuing to perform and document a review of all [redacted] accounts in accordance with DHS policy, including supervisor verification of all access privileges granted through the submission of a new FEMA Form 20-24 by all federal employees and contractors.		**X**	**High**
FEMA-IT-08-06	We noted that FEMA has made a management decision not to develop policies and procedures over the modification of [redacted] account functions until the new [redacted] system upgrade occurs. We noted that FEMA has reported in the Plan of Action and Milestones 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	We recommend that FEMA develop and implement policies and procedures documenting the process of adding, deleting, and modifying [redacted] system functions to ensure that the proper controls are in place for modifying user account privileges.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	the system to ensure that appropriate privileges are created, documented, and approved for a specific function.				
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 [redacted] was present for a majority of the fiscal year.	• Dedicate resources to complete the review of [redacted] user access for FY 2008 and conduct subsequent annual reviews of [redacted] user access by performing the management certification process in accordance with FEMA and DHS policies and procedures. • Fully implement the policies and procedures in place for the [redacted] recertification process and retain auditable records, in accordance with DHS policy, that provide evidence that recertifications are conducted and completed periodically with timeliness.		**X**	**Medium**
FEMA-IT-08-13	KPMG was informed that terminated [redacted] users are to have the "[redacted]" 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 [redacted] access privileges cancelled and their user account removed. Consequently, although the risk is mitigated by the limited access rights on the accounts with the "[redacted]" privilege, those six accounts demonstrate that the policies and procedures surrounding the [redacted] terminated user process are not consistently applied and the accounts	Ensure that policies and procedures over removal of separated user access to [redacted] and [redacted] are consistently followed by removing accounts for any separated users immediately upon notification of separation according to FEMA, DHS and National Institute of Standards and Technology guidance.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	have not been removed. Additionally, four (4) out of the ten (10) accounts remained on the [redacted] system with an active status.				
FEMA-IT-08-17	There is no documented evidence to support that monitoring of the "[redacted] directory and sub-directories of [redacted] is occurring.	We recommend that FEMA establish a process within existing procedures for retaining documented evidence that the "[redacted]" directory and sub-directories are being monitored to verify that only authorized changes are implemented into production.		**X**	**Medium**
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.	We recommend that FEMA's process for monitoring sensitive access and suspicious activity on [redacted] system software include retention of evidence that audit records are proactively reviewed.		**X**	**Medium**
FEMA-IT-08-22	Per inspection of the Plan of Actions and Milestones, we noted that corrective action was initiated by FEMA to implement an alternate processing facility for [redacted] 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 twelve (12) months. Consistent with DHS policy for corrective actions that cannot be implemented within twelve (12) months, a DHS IT Security Program Waiver (number WR-2008-012) was approved by the DHS Chief Information Security Officer in March 2008 to provide FEMA with additional time to plan and	• Complete on-going efforts to fully establish and implement an alternate processing site for the [redacted] system according to DHS 4300A. • Ensure that redundant servers are created at the alternate processing site that is established for the [redacted] servers located at the [redacted] during implementation of the alternate processing site. • Update the existing waiver, as required, in accordance with effective DHS policy		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	develop an effective alternate processing site for [redacted]. Per DHS policy, the waiver must be reviewed, updated, and re-approved by the appropriate management officials every six (6) 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 [redacted] data and offsite backup storage are performed. However, a fully successful table-top test of [redacted] 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.	regarding waivers, and ensure that compensating controls described in the waiver are effective and documentation of their effectiveness is maintained as auditable records.			
FEMA-IT-08-23	[redacted] 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.	We recommend that FEMA develop and implement procedures to periodically test the [redacted] backups in accordance with DHS Information Technology Security Program Publication 4300A requirements.		**X**	**Low**
FEMA IT-08-24	We noted that the tape restore schedule requires quarterly testing of backup tapes beginning no earlier than FY 2009.	We recommend that FEMA periodically test [redacted] backups on a quarterly basis in compliance with FEMA and DHS policy.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	Additionally, we determined that the Contingency Plan was not tested and consequently a full backup tape restore did not occur in FY 2008. Rather, system administrators conducted ad hoc backup tape restores at the request of system users during the fiscal year.				
FEMA-IT-08-25	Due to the magnitude of the project scope to establish a "real-time" alternate processing site for FEMA was unable to implement corrective actions to fully remediate the prior year finding within twelve (12) months. Consistent with DHS policy for findings that cannot be remediated within twelve (12) months, a DHS IT Security Program Waiver (number WR-2008-012) was approved by the DHS Chief Information Security Officer in March 2008 to provide FEMA with additional time to plan and develop an effective alternate processing site for Per DHS policy, the waiver must be reviewed, updated, and re-approved by the appropriate management officials every six (6) 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 the	• Continue to dedicate resources towards completing on-going corrective actions to implement a "real-time" alternate processing site for • Update the existing waiver, as required, in accordance with effective DHS policy regarding waivers, and ensure that compensating controls described in the waiver are effective and documentation of their effectiveness is maintained as auditable records. • In the event that an updated waiver is denied or when the alternate processing site is established, conduct documented annual tests of the contingency plan that address all critical phases of the plan. • Update the contingency plan based on the lessons learned from table-top or full-scale testing results, as necessary.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	[redacted] 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-08-28	During our FY 2008 follow up test work, we tested a selection of 40 [redacted] non-emergency application level [redacted] that had occurred since October 1, 2007. Of the 40 [redacted] tested, we noted the following exceptions: • 29 [redacted] did not have testing documentation attached to the [redacted]; • 36 [redacted] did not have [redacted] approval; and • 32 [redacted] did not have [redacted] approval	We recommend that FEMA, in accordance with DHS and FEMA policy, ensure that [redacted] non-emergency application level changes obtain all required approvals prior to implementation into production and that testing documentation is appropriately retained.		X	**Medium**
FEMA-IT-08-29	We noted that [redacted] approvals for [redacted] application level emergency changes did not consistently follow FEMA and DHS guidance. Specifically, we determined that of 25 emergency [redacted] changes selected for testing: • 22 changes did not have documented [redacted] approval; • 4 did not have [redacted] approval prior to	We recommend that FEMA, in accordance with DHS and FEMA policy, ensure that [redacted] application level emergency changes obtain all required approvals prior to implementation into production and that testing documentation is appropriately retained.		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	implementation into production; • 16 did not have [redacted] approval; and • 6 did not have related testing documentation attached.				
FEMA-IT-08-38	We were referred to Section 2.2.1 of the NFIP [redacted] 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 [redacted] Additionally, while we noted that system roles and responsibilities have been documented, [redacted] duties that are incompatible are not documented.	We recommend that NFIP document [redacted] duties that are incompatible and develop and implement policies and procedures for properly segregating incompatible duties within the system.		**X**	**Medium**
FEMA-IT-08-39	During our test work, we noted that a planned update and subsequent testing of the [redacted] Contingency Plan was not conducted and that system fail-over capability at the alternate processing site had not been tested Additionally the NFIP [redacted]) was not updated to include the [redacted] and [redacted] alternate processing facility or [redacted] critical data files and restoration priorities.	• Update and test the [redacted] Contingency Plan, covering all critical phases of the plan in accordance with DHS policy. In addition, NFIP should conduct a test of the system fail-over capability at the alternate processing site. • Revise the Disaster Recovery and [redacted] to incorporate the [redacted] and [redacted] alternate processing facility and the [redacted] critical data files, as well as update the plans with lessons learned from the testing.		**X**	**Medium**
FEMA-IT-08-45	[redacted] user access is not managed in accordance with account management procedures.	• In support of the OCFO Procedures for Granting Access to [redacted] continue to ensure the process for granting or modifying access is monitored and that changes made to user profiles outside of the recertification	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
		process are documented and authorized by supervisors, program managers, and Contracting Officer's Technical Representatives. • Ensure that the [redacted] Database User Access Instruction is implemented consistently by requiring that all existing and new [redacted] users complete a current [redacted] Database User Access Form. • Complete the development and implementation of policies and procedures over periodic recertification of all user access to the [redacted] [redacted] database, and retain auditable records in accordance with DHS polices and procedures as evidence that recertifications are conducted and completed periodically with timeliness.			
FEMA-IT-08-46	The existing Memorandum of Understanding (MOU) with the Department of Treasury expired in October 2007.	We recommend that FEMA complete the review, reauthorization, and re-issuance of a current MOU and Interconnection Security Agreement (ISA) between the Treasury's Financial Management Service and FEMA.	X		**Low**
FEMA-IT-08-47	Based upon our review, we determined that the ISA between FEMA and the Small Business Administration (SBA) expired in July 2007 and has not been reauthorized and reissued, as required by DHS policy.	Complete the reauthorization and reissuance of a renewed ISA between FEMA and SBA, and ensure that the ISA is subsequently reviewed, updated as necessary, and reissued timely, as required by DHS policy and/or the terms of the agreement.	X		**Low**
FEMA-IT-08-	The vulnerabilities identified from the [redacted] scans	We recommend that FEMA implement a process	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
48	are not reported and tracked via DHS' POA&M process.	to ensure that weaknesses identified during vulnerability assessment scans of [redacted] are formally reported and that associated corrective actions are developed and tracked via DHS' POA&M process.			
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: • [redacted] for automatically scanning system files for threats, known viruses, and worms on a continuous basis when Windows is started; • [redacted] for automatically scanning Outlook and/or Outlook Express messages for viruses. • [redacted] for automatically scanning incoming and outgoing Lotus Notes messages; and • [redacted] for scanning all incoming and outgoing e-mail messages other than Outlook and/or Outlook Express.	Action was taken to correct this weakness during the audit period. No further recommendation is required.	X		**Medium**
FEMA-IT-08-50	• On a daily basis, an automated report of [redacted] database activity conducted by users with elevated "superuser" privileges is generated and emailed to the Database Administrators (DBA) and FSS personnel for review. However, while this report is distributed for review by the DBAs and FSS staff, no evidence that the reviews are conducted is retained.	We recommend that FEMA, in accordance with FEMA and DHS policy, continue to implement procedures over audit logging processes for the [redacted] application and database and retain evidence that audit records are proactively reviewed. Specifically, the evidence should provide a record of review that at a minimum notes the identity of the individual that reviewed the log (e.g., initials), the date of review, and	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	- We noted that while FEMA Instruction 2200.7, [redacted] *User Access Instruction*, assigns the responsibility of conducting this weekly review to FSS, FEMA personnel do not formally document that the review is conducted.	follow up actions taken, if required.			
FEMA-IT-08-51	- We noted that the Standard Operating Procedures (SOP) for Handling of [redacted] Audit Logs does not comprehensively address requirements of FEMA Directive 140-1, FEMA Information Technology Security Policy. Specifically, the SOP does not require the monitoring of modifications to account tables and other highly-privileged and administrator-level activities. - 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.	We recommend that FEMA revise existing procedures for [redacted] audit logging to include a review of highly-privileged and administrator-level activities as required by FEMA and DHS policy and ensure implementation of all requirements, including retention of evidence of reviews of audit logs.	**X**		**High**
FEMA-IT-08-52	Existing procedures do not provide a timeframe for installing [redacted] patches. Finalization and implementation of the [redacted] - FEMA Information Security Vulnerability Management, which specifies the timeframe for installing security patches, has been delayed due to organizational changes.	We recommend that FEMA finalize and implement procedures that define the timeframe in which security patches should be installed.	**X**		**Medium**
FEMA-IT-08-	Upon inspection of the [redacted] System Security Plan	We recommend that FEMA ensure that [redacted]	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
53	(SSP) that is a part of the [redacted] 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.	SSP is updated in accordance with DHS policy so that current system components and system owners are comprehensively documented in the plan.			
FEMA-IT-08-54	In FY 2008, we determined that NFIP had documented and implemented the [redacted] System Change Control Procedures. During the audit, we determined that two (2) [redacted] 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.	We recommend that NFIP ensure that testing documentation for [redacted] changes is retained on file in accordance with DHS policy.	**X**		**Medium**
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 (8) [redacted] changes that had been implemented since October 1, 2007. Of the eight (8) tested, we identified that test results were not available for one (1) change.	We recommend that NFIP ensure that testing of all changes is documented and retained on file in accordance with DHS and NFIP requirements.	**X**		**Medium**

*** Risk ratings are only intended to assist management in prioritizing corrective actions. Risk ratings in this context do not correlate to definitions of control deficiencies as identified by the AICPA.**

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison To Current Year Notices of Findings and Recommendations

Department of Homeland Security
Federal Emergency Management Agency

Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
FEMA-IT-07-01	During our technical testing, patch management weaknesses were identified on Integrated [redacted], and [redacted] systems.	X	
FEMA-IT-07-02	During our technical testing, configuration management weaknesses were identified on [redacted], [redacted] [redacted] and key support servers.		FEMA-IT-08-02
FEMA-IT-07-03	We determined that the Financial Services Section (FSS) has created procedures to review [redacted] user access on a semi-annual basis for appropriateness of access privileges granted to employees or contractors within their organization. Additionally, we noted that a recertification of all [redacted] users, which is also their semi-annual review of user access, began in June 2007. Currently, FSS is in the process of validating [redacted] access for users who responded to FSS' recertification request. In addition, FSS is locking out the [redacted] users who did not respond. We determined that the recertification of all existing [redacted] users has not been completed for FY 2007.		FEMA-IT-08-03
FEMA-IT-07-04	The FEMA alternate processing site located in [redacted] is not operational for [redacted] FEMA is in the process of setting up a [redacted]) to replicate data from the [redacted] production server at [redacted] and send it to the [redacted] servers in [redacted]. Currently the [redacted] is not complete and therefore, the [redacted] facility does not have the capability of functioning as the alternate processing site for [redacted] if a disaster were to occur.	X	
FEMA-IT-07-05	The [redacted] Security Test & Evaluation did not provide adequate documentation of the results to the accrediting authority and that the prior year weakness still exists.	X	
FEMA-IT-07-06	There are not formal, documented procedures in place to require updates to the [redacted] system documentation as [redacted] functions are added, deleted, or modified.		FEMA-IT-08-06
FEMA-IT-07-07	We determined that FEMA has identified the [redacted]) as the alternate processing facility for [redacted]; however, it will not be fully operational until September 2007. Therefore, we determined that the [redacted] contingency plan has not undergone a full-scale test to show that the system can be brought back to an operational state at the designated alternate site.	X	
FEMA-IT-07-08	We determined that the FEMA [redacted] has not been updated to include the new listing of FEMA mission critical IT systems as outlined in the Information Technology Services Directorate [redacted]	X	

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	Description	Closed	Repeat
	Implementation Plan.		
FEMA-IT-07-09	We noted that FEMA has begun to standardize all user workstations to [redacted] with [redacted] installed, which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to [redacted] or providing users with new workstations. However, we noted that this process will not be fully complete until January 2008. This weakness impacts [redacted] We noted that FEMA users are locked out of the system at the domain level after three (3) consecutive failed login attempts; however, the user account becomes unlocked and active again after five (5) minutes of inactivity.	X	
FEMA-IT-07-10	We determined that FEMA has begun to standardize all user workstations to [redacted] with [redacted] installed, which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to [redacted] or providing users with new workstations. However, we noted that this process is not fully completed, and FEMA has estimated this process will not be completed until January 2008. This weakness impacts [redacted]	X	
FEMA-IT-07-11	We noted that passwords for the [redacted] application can be re-used after six (6) iterations which is not in compliance with DHS 4300A.	X	
FEMA-IT-07-12	We determined that the FEMA Chief Information Officer (CIO) provided procedures to all Office Directors, Regional Directors and FEMA Coordinating Officers for the periodic review of all [redacted] accounts and position assignments on June 28, 2007. We noted that detailed procedures are listed for the review of [redacted] accounts; however, the procedures do not state the frequency of this review. We noted that this review began on June 29, 2007 with a deadline of July 26, 2007 for accepting responses from users recertifying their [redacted] accounts. Therefore, risk of unauthorized users accessing [redacted] was present for a majority of the fiscal year.		FEMA-IT-08-12
FEMA-IT-07-13	We determined that the FSS has created procedures to review [redacted] user access on a semi-annual basis for appropriateness of access privileges granted to employees or contractors within their organization. Additionally, we noted that a recertification of all [redacted] users was performed in June 2007.		FEMA-IT-08-13

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	Currently, FSS is in the process of validating [redacted] access for the users who responded to FSS' recertification request and locking out the [redacted] users who did not respond. We determined that the recertification of all existing [redacted] users is not yet complete for FY 2007. We determined that the FEMA CIO provided procedures to all Office Directors, Regional Directors and FEMA Coordinating Officers for the periodic review of all [redacted] accounts and position assignments on June 28, 2007. However, the procedures do not state the frequency of this review. Furthermore, we noted that this review began on June 29, 2007 with a deadline of July 26, 2007 for accepting responses from users recertifying their [redacted] accounts. Therefore, the risk of unauthorized users accessing [redacted] was present for a majority of the fiscal year. We noted that twenty-seven (27) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts. We noted that seven hundred seventy (770) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts.		
FEMA-IT-07-14	We determined that IT Operations has created backup procedures entitled, [redacted], for [redacted] and [redacted] dated July 27, 2007. However, we noted that the procedures were finalized on July 27, 2007, and that the risk was present for a majority of the fiscal year. We noted that both [redacted] and [redacted] backup tapes are not rotated off-site to the [redacted]. We noted that the FEMA alternate processing site located in [redacted] is not operational for [redacted] We also noted that the [redacted] back-up facility has redundant servers in place for the [redacted] [redacted] Database in June 2007. Therefore, the risk was present for a majority of the fiscal year.	X	
FEMA-IT-07-15	We determined that FEMA created the [redacted] [redacted] [redacted], [redacted], dated June 29, 2007. We noted that this plan was in draft form and that it does not fully identify the configuration management process of [redacted] We determined that FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B, which details policies for restricting access to the system software of FEMA IT systems. However, we noted that the draft policy is dated June 14, 2007. We noted that procedures over restricting access to [redacted] system software	X	

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	entitled, [redacted] Procedures, and [redacted] patch management procedures were approved on June 29, 2007. However, we noted that the risk was present for a majority of the fiscal year, and as a result, the NFR will be re-issued for FY 2007.		
FEMA-IT-07-16	FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B, which details policies for restricting access to system software. However, we noted that the policy is in draft and dated June 14, 2007. FEMA has not documented procedures for restricting access to [redacted] system software.	X	
FEMA-IT-07-17	We determined that FEMA created a [redacted] Standard Operating Procedures (SOP) for [redacted] However, the [redacted] SOP was approved by the OCFO on June 29, 2007. Furthermore, we noted the evidence that the "[redacted]" account was locked within the [redacted] environment on July 24, 2007. Therefore, we noted that the risk was present for a majority of the fiscal year.		FEMA-IT-08-17
FEMA-IT-07-18	FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B detailed policies for investigating and reporting any suspicious activity detected when reviewing audit logs. However, we noted that the policy is dated June 14, 2007 and is in draft form. FEMA has not documented specific procedures to review suspicious system software activity and access controls for [redacted]	X	
FEMA-IT-07-19	FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B detailed policies for monitoring sensitive access and investigating and reporting any suspicious activity detected when reviewing audit logs. However, we noted that the policy is dated June 14, 2007 and is in draft form. FEMA has not documented procedures to monitor and review sensitive access, system software utilities and suspicious system software and access activities for [redacted]		FEMA-IT-08-19
FEMA-IT-07-20	FEMA has adopted the DHS [redacted] for [redacted] This policy establishes required practices for managing DHS IT systems and infrastructure solutions through a progression of activities for initiation, planning, development, testing, implementation, operation, maintenance, and retirement. However, we noted that the policy is dated January 27, 2006 and is in draft form.	X	

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
FEMA-IT-07-21	FEMA has adopted the DHS [redacted] for [redacted] This policy establishes required practices for managing DHS IT systems and infrastructure solutions through a progression of activities for initiation, planning, development, testing, implementation, operation, maintenance, and retirement. However, we noted that the policy is dated January 27, 2006 and is in draft form.	X	
FEMA-IT-07-22	FEMA did not have an operational alternate processing site for [redacted] for a majority of the fiscal year. We determined that the alternate processing site in [redacted] has redundant servers in place for the [redacted] [redacted] Database effective as of June 2007.		FEMA-IT-08-22
FEMA-IT-07-23	FEMA lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.		FEMA-IT-08-23
FEMA-IT-07-24	FEMA lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.		FEMA-IT-08-24
FEMA-IT-07-25	We noted that the [redacted] contingency plan has not been tested on an annual basis, per DHS 4300A.		FEMA-IT-08-25
FEMA-IT-07-26	During our review of user access rights for the approval of [redacted] [redacted] [redacted] we noted that excessive access rights existed. Specifically, we determined that three (3) people were authorized to approve [redacted] [redacted] [redacted]s; however, one (1) individual was transferred to another DHS agency. Therefore, this person's job responsibilities no longer required this access nor was this individual a current FEMA employee. Upon notification of this issue, FEMA took corrective action and removed the individual's access rights.	X	
FEMA-IT-07-27	We noted that testing documentation for [redacted] application level changes is not consistently documented or performed timely.	X	
FEMA-IT-07-28	Per DHS 4300A, all changes to major applications must be formally approved, tested and documented prior to the change being implemented. For the test of this control, we selected a sample of nine (9) [redacted] application level changes. We noted that one (1) out of the sample did not have testing performed.		FEMA-IT-08-28
FEMA-IT-07-29	We noted that the Technical Review Committee ([redacted]) approvals for [redacted] application level emergency changes are not consistently documented. Specifically, we determined that five (5) out of a sample of eight (8) [redacted] application level emergency changes did not gain [redacted] approval.		FEMA-IT-08-29

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	Description	Closed	Repeat
FEMA-IT-07-30	We determined that excessive access is designed to be permitted within [redacted] to make offline changes to the general ledger account tables via the [redacted] Group. We identified six (6) users in the [redacted] group that have the ability to make offline changes to the general ledger account tables, which are not within their job responsibilities.	X	
FEMA-IT-07-31	[redacted] does not timeout after a period of inactivity. Additionally, we determined that all [redacted] workstations use a password protected screensaver after fifteen (15) minutes of inactivity, which is not in compliance with DHS 4300A. [redacted] access is not reviewed on a periodic basis to determine if access is valid and commensurate with job responsibilities.	X	
FEMA-IT-07-32	While a standard form has been developed for documenting [redacted] change requests, [redacted] change management procedures have not been documented. System software change management procedures have not been developed or implemented. Additionally, installation of the operating system upgrade in FY 2007 was not formally documented or approved.	X	
FEMA-IT-07-33	NFIP has made improvements in the area of Administrator account management. However, we noted that system activity logs are not being reviewed.	X	
FEMA-IT-07-34	NFIP has updated the [redacted] baseline configuration document. However, we noted that procedures have not been developed which require approvals prior to implementation. Additionally, of 30 changes selected, 14 changes did not have documented Operations Service Request forms or documented approvals.	X	
FEMA-IT-07-35	A system programmer [redacted] had write access to the [redacted] [redacted] and [redacted] [redacted] datasets of the [redacted] production member. NFIP removed the system programmer's access shortly after this finding was identified.	X	
FEMA-IT-07-36	Access to the [redacted] excel files is excessive. Specifically, we identified that modify and write access permissions to the excel files are inappropriate for five individuals of the Bureau of Finance and Statistical Control group.	X	

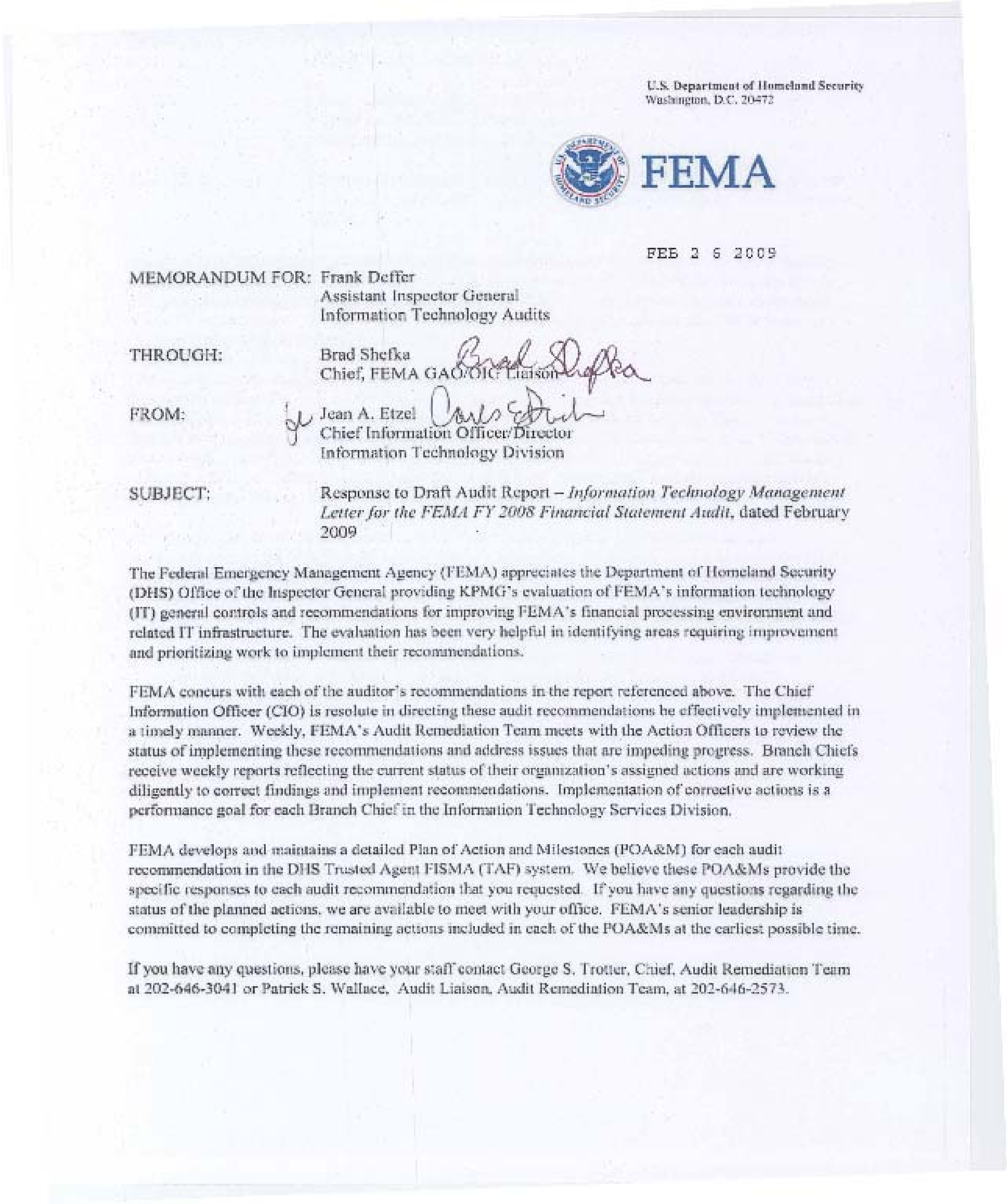
Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	Description	Closed	Repeat
FEMA-IT-07-37	We noted there is excessive access to [redacted] application software and support files. Specifically, we noted that all individuals within the Bureau of Finance and Statistical Control group have modify and write access to the [redacted] application software and support files.	X	
FEMA-IT-07-38	NFIP has not documented incompatible duties within [redacted] developed policy and procedures regarding segregation of duties, or implemented segregation of duties controls within [redacted]. All users of [redacted] have full application level access.		FEMA-IT-08-38
FEMA-IT-07-39	The [redacted] contingency plan has not been tested. As a result, the system fail-over capability for the [redacted] alternate processing site has not been tested. The NFIP Disaster Recovery and COOP does not identify the following: The [redacted] and [redacted] alternate processing facility; and [redacted] critical data files are not documented.		FEMA-IT-08-39
FEMA-IT-07-40	The rules of behavior (ROB) forms are not consistently signed prior to users gaining access to the NFIP Bureau [redacted]). Specifically, we determined that three (3) out of a sample of twelve (12) new NFIP Bureau [redacted] users did not sign the ROB prior to obtaining NFIP Bureau [redacted] access.	X	
FEMA-IT-07-41	We determined that policies and procedures over periodic review of [redacted] access lists have been documented. However, we noted that the periodic review determining if logical user access is valid and consistent with job responsibilities is not effective as an instance of excessive system developer access was identified within [redacted]	X	
FEMA-IT-07-42	We determined that periodic review policies and procedures have not been developed for access to the NFIP Bureau [redacted] room. As a result, we noted that there are two (2) employees with excessive access to the NFIP Bureau [redacted] room.	X	
FEMA-IT-07-43	The NFIP Bureau [redacted] has been configured to permit users to reuse prior passwords after five (5) iterations which is not in compliance with the DHS 4300A.	X	
FEMA-IT-07-44	We noted that proactive vulnerability scanning is not performed over [redacted] backend database or the NFIP Bureau [redacted].	X	

Appendix D

Management Comments

Department of Homeland Security
Federal Emergency Management Agency
Information Technology Management Letter
September 30, 2008



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

FEMA

FEB 2 6 2009

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
Information Technology Division

SUBJECT: Response to Draft Audit Report – *Information Technology Management Letter for the FEMA FY 2008 Financial Statement Audit*, dated February 2009

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 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. Weekly, FEMA's Audit Remediation Team meets with the Action Officers to review the status of implementing these recommendations and address issues that are impeding progress. Branch Chiefs receive weekly reports reflecting the current status of their organization's assigned actions and are working diligently to correct findings and implement recommendations. Implementation of corrective actions is a performance goal for each Branch Chief in the Information Technology Services Division.

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 George S. Trotter, Chief, Audit Remediation Team at 202-646-3041 or Patrick S. Wallace, Audit Liaison, Audit Remediation Team, at 202-646-2573.

Report Distribution

Department of Homeland Security

Secretary
Acting Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
Under Secretary, Management
Acting 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) 254-4199, 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.