DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FEMA Component of the FY 2007 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-08-68

June 2008

Office of Inspector General

U.S. Department of
Homeland Security
Washington, DC 20528

June 27, 2008

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the Federal Emergency Management Agency (FEMA) component of the DHS financial statement audit as of September 30, 2007. 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-08-12, November 2007) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of FEMA's FY 2007 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 14, 2008, 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. It is our hope 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

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 14, 2007

Inspector General
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) as of September 30, 2007, 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, 2007 (referred to herein as "other financial statements"). Because of matters discussed in our *Independent Auditors' Report*, dated November 15, 2007, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements. As part of this engagement, we performed certain procedures at the DHS Federal Emergency Management Agency (FEMA) as of September 30, 2007.

In connection with our fiscal year 2007 engagement, we were also engaged to consider FEMA's internal control over financial reporting and to test FEMA's compliance with certain provisions of applicable laws, regulations, contracts, and grants that could have a direct and material effect on the DHS financial statements. Our procedures do not include examining the effectiveness of internal control and do not provide assurance on internal control. We have not considered internal control since the date of our report.

We noted certain matters involving internal control and other operational matters with respect to information technology that are summarized and presented in Exhibit A for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and have been communicated through the issued Notices of Finding and Recommendation (NFR), are intended to improve information technology internal control or result in other operating efficiencies and are intended **For Official Use Only**. Exhibits B and C present additional information for management's use. Our findings involving internal control and other operational matters noted that do not relate to information technology have been presented in our *Independent Auditors' Report*, dated November 15, 2007, and in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated December 21, 2007.

Our audit procedures were designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies and procedures that may exist. We aim, however, to use our knowledge of FEMA's organization gained during our work to make comments and suggestions that we hope will be useful to you.

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

This report is intended for the information and use of FEMA and DHS management, the Office of the Inspector General, the U.S. Office of Management and Budget, the U.S. Congress, and the Government Accountability Office, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Federal Emergency Management Agency
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement

INFORMATION TECHNOLOGY MANAGEMENT LETTER

Table of Contents

Exhibit A

OBJECTIVE, SCOPE AND APPROACH

We performed audit procedures over the FEMA general controls in support of the FY 2007 DHS financial statement audit engagement. The overall objective of our audit procedures was to evaluate the effectiveness of information technology (IT) general controls of FEMA's 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, formed the basis of our audit procedures. Further information related to the scope of the FEMA's IT general controls assessment is described in Exhibit B.

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 general IT controls environment.

- *Entity-wide security program planning and management* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control* – 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* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software* – Controls that limit and monitor access to powerful programs that operate computer hardware.
- *Segregation of duties* – 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* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit procedures, we also performed technical security testing for key network and system devices. The technical security testing was performed 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 general control environment, we performed application control tests 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, or payroll.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Our audit procedures over IT general controls for FEMA included testing of its procedures, policies, and practices. The scope of our testing included the general and application controls at FEMA Headquarters, the National Flood Insurance Program (NFIP), [redacted] and, as of April 1, 2007, the former Office of Grants and Training (G&T).

During FY 2007, there were ten (10) FEMA prior year findings that were properly closed primarily in access controls, entity-wide security planning, and application controls. Also during the year, FEMA took steps to address other known weaknesses, such as drafting new policies and procedures, developing a process to recertify application users, and beginning domain level upgrades to user workstations. Despite the initiation of various improvements, our test work resulted in the reissuance of 31 prior year findings and the issuance of 13 new findings. These issues collectively limit FEMA's ability to ensure that critical financial and operational data is maintained in a manner to ensure confidentiality, integrity, and availability. Consequently, these weaknesses negatively impacted the internal controls over FEMA financial reporting and its operation.

FEMA management should place a strong emphasis on the monitoring and enforcement of IT security-related policies and procedures. Ongoing measures to improve the IT security considerations for key financial systems and effective access controls, service continuity, change controls, system software, and entity-wide security are needed. Additionally, many of the repeat vulnerabilities identified during technical security testing can be addressed by ensuring that the system configurations associated with the builds, service packs, and software patches are in compliance with DHS and the National Institute of Standards and Technology (NIST) standards.

Federal Emergency Management Agency
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement
Exhibit A

IT GENERAL CONTROL FINDINGS BY AREA

A. Entity-wide Security Program Planning and Management

During FY 2007, we noted a weakness in the entity-wide security program planning and management. Specifically, the [redacted] Security Test & Evaluation (ST&E) did not provide adequate documentation of the results to the accrediting authority and that the prior year weakness still exists.

Recommendation:

We recommend that the FEMA Chief Financial Officer (CFO) and Chief Information Officer (CIO) offices ensure the following corrective actions are implemented:

1. Document the results of the [redacted] ST&E by providing a detailed listing for the vulnerabilities and/or corrective action for the vulnerabilities in the authority to operate (ATO) and documenting them in an individual manner in the Plan of Actions and Milestones (POA&M) when the system is re-certified and accredited in FY 2008.

B. Access Controls

During FY 2007, access control weaknesses were identified as a result of the general controls and vulnerability testing. These are important weaknesses to correct because they allow personnel inside the organization who best understand the organization's systems, applications, and business processes are able to obtain unauthorized access to FEMA data.

We noted the following weaknesses related to access controls that impact FEMA's financial processing:

- During our technical testing, patch management and configuration weaknesses were identified on [redacted] and the [redacted] and key support servers.
- The following [redacted] access control weaknesses were identified:
  - User recertification for access to [redacted] has not been completed.
  - User access is not removed in a timely manner.
    - We noted that 27 terminated or separated FEMA employees and contractors maintain active [redacted] user accounts.
    - We noted that 770 terminated or separated FEMA employees and contractors maintain active [redacted] user accounts.
  - Access to [redacted] are not effectively controlled and needs improvement, as evidenced by the following:
    - Weak password management is maintained for [redacted].
    - Security screen lockout is not in compliance with DHS policy.
    - [redacted] user access is not recertified on a regular basis.
  - Policies and procedures over access to [redacted] system software have not been developed.
- Excessive access to the [redacted] room exists.
- [redacted] access controls need improvement; specifically, we noted:
  - [redacted] does not timeout after a period of inactivity. Additionally, we determined that all NFIP workstations use a password protected screensaver after 15 minutes of inactivity, which

is not in compliance with DHS *IT Security Program Sensitive System Handbook,* 4300A.

- [redacted] access is not reviewed on a periodic basis to determine if access is valid and commensurate with job responsibilities.
- Excessive access exists within the [redacted]) application housed at NFIP.
- Excessive access exists to the Loss Adjustment Expense (LAE) Excel files. Specifically, we identified that modify and write access permissions to the Excel files are inappropriate for five individuals.
- [redacted] password configurations need improvement.
- Vulnerability scanning is not performed over [redacted] backend database or the [redacted].

Recommendations:

We recommend that the FEMA CFO and CIO offices ensure the following corrective actions are implemented:

1. Implement the corrective actions for each of the weaknesses identified during the vulnerability assessment testing as listed in the specific NFR.
2. Complete the recertification of [redacted] user access by removing the access of individuals who did not complete FEMA Form 20-24[redacted] *Access Control Form*, and validate the existing [redacted] user access of individuals who completed FEMA Form 20-24.
3. Implement the Office of Chief Financial Officer (OCFO) Procedures for Granting Access to [redacted] by continuing to perform a review of all [redacted] access on a semi-annual basis including verifying the access privileges granted to federal employees and contractors.
4. Complete implementation of procedures regarding the periodic review of [redacted] access lists, including a review of accounts on a semi-annual basis and removal of terminated employees' access to all FEMA systems.
5. Continue development of the automated process of granting, removing, and validating [redacted] user access and implement by March 2008, per the FY 2006 FEMA IT Financial Audit Remediation Plan.
6. Continue upgrade of all FEMA domain level user's workstations operating system to Windows XP with Service Pack 2 installed and ensure that all [redacted] settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver.
7. Ensure that FEMA users locked out of the system at the domain level after three consecutive failed login attempts remain locked for 20 minutes, per DHS *IT Security Program Sensitive System Handbook, 4300A*.
8. Configure the [redacted] application to require passwords to not be reused until eight (8) iterations have passed to be in compliance with DHS *IT Security Program*, 4300A.
9. Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B.
10. Develop and implement specific procedures for restricting access to [redacted] system software, and promulgate it to all needed personnel, to be in compliance with DHS *IT Security Program Sensitive System Handbook*, 4300A.
11. Develop and implement policies and procedures to periodically review physical access listings over the [redacted] room to determine if access is still required or if access levels are commensurate with users' job responsibilities.
12. Configure the NFIP domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with DHS *IT Security Program Sensitive System Handbook*, 4300A.

13. Develop and implement policies and procedures regarding periodic review of [redacted] and [redacted] access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege.
14. Restrict access to the LAE Excel files to the Actuary and Finance Director in order to achieve the principle of least privilege.
15. Ensure that the [redacted] is configured to require passwords to not be reused until eight (8) iterations have passed in order to be in compliance with DHS *IT Security Program*, 4300A.
16. Perform vulnerability scans over the [redacted] backend database and the [redacted] on an annual basis.

C. Application Software Development and Change Control

During FY 2007, we noted weaknesses related to application software development and change control. Specifically, conditions noted that impact FEMA's financial processing are as follows:

- [redacted] configuration management needs improvement. The following policies and procedures have not been authorized or implemented across the FEMA enterprise and remain in draft form:
  - [redacted] Configuration Management Plan, Version 0.1.
  - Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B.
- A System Development Life Cycle (SDLC) for [redacted] has not been finalized.
- Procedures have not been developed which require approvals prior to implementation of changes to the [redacted] mainframe. We found that of 30 changes selected, 14 changes did not have documented Operations Service Request (OSR) forms or documented approvals.
- Excessive approval authority for [redacted] change requests exists.
- [redacted] testing documentation for application level changes is not consistently documented or performed timely.
- [redacted] configuration management testing needs improvement. Specifically, we found that the testing of application changes is not consistent.
- The [redacted] patch management and *Database Administration Access* procedures have been developed, but not implemented.
- The Technical Review Committee (TRC) approvals for [redacted] application level emergency changes are not consistently documented. Specifically, we determined that five (5) of a sample of eight (8) [redacted] application level emergency changes did not gain TRC approval.
- Excessive access to [redacted] application software and support files exists.

Recommendations:

We recommend that the FEMA CFO and CIO offices ensure the following corrective actions are implemented:

1. Finalize and implement the [redacted] Configuration Management Plan to be in compliance with DHS *IT Security Program Sensitive System Handbook*, 4300A.
2. Finalize and implement the Supplemental Security Policy to the DHS *Sensitive Systems Policy Directive* 4300A and 4300B.
3. Implement the *Database Administration Access* procedures and [redacted] patch management procedures.
4. Implement the DHS SDLC for [redacted] program development when DHS finalizes the document. Additionally, FEMA should ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation

process.

5. Ensure that the NFIP Bureau and Statistical Agent documents and implements change management procedures requiring approvals prior to implementing changes in the [redacted] production environment.
6. Develop a process to periodically review user access for the approval of [redacted] system change requests to determine if access is needed.
7. Ensure all [redacted] application level changes are tested in a timely manner.
8. Ensure all test data and transactions are appropriately documented and maintained with the respective system change request within the system.
9. Ensure all [redacted] application level emergency changes obtain TRC approval prior to being implemented into the production environment.
10. Remove excessive access to the [redacted] application software and support files.
11. Develop and implement procedures to perform a periodic review of access to [redacted] application software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.

D. System Software

During FY 2007, we noted weaknesses related to system software. Specifically, the conditions noted that impact FEMA's financial processing are as follows:

- Excessive access exists to the [redacted]" directory, which allows system programmers the ability to migrate code into the [redacted] production environment.
- Investigation policies and procedures over [redacted] system software have been developed, but remain in draft.
- Monitoring of [redacted] system software needs improvement.
- [redacted] change management procedures have not been documented for application changes nor system software. In addition, the installation of the operating system upgrade in FY 2007 was not formally documented or approved.
- Excessive access to [redacted] mainframe production datasets exists.

Recommendations:

1. Implement the System Change Request Standard Operating Procedures by keeping the [redacted]" account locked at all times, except when a change needs to be deployed in the IFMIS production environment, and by monitoring the "[redacted]" directory and sub-directories to detect updates.
2. Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B.
3. Develop and implement specific procedures for the review of suspicious system software activity and access controls for [redacted], and promulgate it to all needed personnel.
4. Develop and implement specific procedures to monitor sensitive access and system software utilities for [redacted], and promulgate it to all needed personnel.
5. Document the change management procedures for the [redacted] application.
6. Develop and implement change management procedures for [redacted] system software changes and establish documented approvals prior to installing or upgrading system software.
7. Ensure that the [redacted] Bureau and Statistical Agent develops and implements procedures to perform a periodic review of access to [redacted] mainframe production datasets to determine whether access is valid, consistent with job responsibilities, and conformed to the least privilege principle.

Exhibit A

E. Service Continuity

During FY 2007, we noted weaknesses related to service continuity. Specifically, conditions noted that impact FEMA's financial processing are as follows:

- The [redacted] lacks an alternative processing center.
- [redacted] controls over backup tapes need improvement. We noted that FEMA lacks backup testing procedures and that the backup tapes are not periodically tested.
- An alternate processing site for [redacted] has not been established.
- The [redacted] contingency plan has not been tested on an annual basis.
- The [redacted] contingency plan testing needs improvement.
- FEMA's Continuity of Operation Plan (COOP) has not been updated to include the new listing of FEMA mission critical IT systems as outlined in the Information Technology Service Division (ITSD) COOP Implementation Plan.
- The [redacted] contingency plan has not been tested, and the [redacted] Disaster Recovery and COOP needs improvement.
- The Rules of Behavior forms are not consistently signed prior to users gaining access to the [redacted]. Specifically, we determined that three (3) of a sample of 12 new [redacted] users did not sign the Rules of Behavior prior to obtaining [redacted] access.

Recommendations:

We recommend that the FEMA CFO and CIO offices ensure the following corrective actions are implemented:

1. Complete efforts to implement the [redacted]) data center's "real-time" back-up facility as its alternate processing site and create redundant servers for the [redacted] servers located at [redacted].
2. Implement the new developed *Backup Media Protection and Control* procedures by performing the [redacted] backups on a regular basis. When performing [redacted] backups, FEMA should:
   - Maintain a documented backup inventory for [redacted].
   - Rotate [redacted] backups off-site to the Virginia NPSC on a regular basis.
   - Log the deposit and withdrawal of [redacted] backup tapes.
   - Ensure that logs are maintained per the stated retention time period.
   - Develop and implement procedures to test the [redacted] backups at least annually in compliance with DHS *IT Security Program Sensitive System Handbook*, 4300A.
3. Perform an annual test of the [redacted] contingency plan, which covers all critical phases of the plan.
4. Perform a full-scale test of the [redacted] contingency plan once the [redacted] data center is operational as the alternate processing site for [redacted]. As a part of the full-scale contingency plan test, FEMA should include the critical IT components, such as key contingency personnel, backup servers at the alternate processing site, and use of backup tapes to bring up the system, in order to assess if they will operate as planned. Additionally, a test of the [redacted] contingency plan should be performed annually.
5. Update the COOP to clearly state and prioritize the listing of 22 mission critical IT systems to be restored at its alternate processing site in the event of a disaster.

Exhibit A

6. Perform a test of the [redacted] contingency plan, covering all critical phases of the plan on an annual basis.
7. Perform a test of the system fail-over capability at the alternate processing site for [redacted].
8. Revise the Disaster Recovery and COOP to incorporate the [redacted] alternate processing facility and the [redacted] critical data files.
9. Ensure that all employees and contractors acknowledge and sign a Rules of Behavior prior to being granted access to the [redacted].

F. Segregation of Duties

During FY 2007, we noted one weakness in segregation of duties. Specifically, the NFIP Bureau and Statistical Agent 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.

Recommendations:

We recommend that the FEMA CFO and CIO offices ensure the following corrective actions are implemented:

1. Identify and document incompatible duties and system roles and responsibilities within [redacted].
2. Develop and implement policies and procedures segregating incompatible duties within [redacted], to be in compliance with DHS *Information Technology Security Program Sensitive System Handbook,* 4300A.
3. Identify and implement capabilities within [redacted] that enforce segregation of incompatible duties.

APPLICATION CONTROL FINDING

We performed application control testwork over the financial reporting process in the [redacted]. We reviewed access over the account mapping functions within [redacted]. The account mapping functions allow a user to change accounting transaction codes and account attributes within [redacted], which then are reflected on the data file that is submitted into the [redacted] during the month-end close.

Excessive access is permitted within [redacted] to make offline changes to the general ledger account tables via the [redacted]. 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.

Due to the nature of FEMA's business, system developers are allowed to have system administrator access so they can bypass various security settings in order to perform their jobs efficiently. This access could allow a person to intentionally or inadvertently use various functions to alter the integrity of the data within the application.

Recommendations:

We recommend that the FEMA CFO and CIO offices ensure the following corrective actions are implemented:

1. Implement a solution to limit the excessive access to make offline changes to the general ledger account tables.
2. Periodically reevaluate access rights and limit access to users who have a business need.

MANAGEMENT COMMENTS AND OIG EVALUATION

We obtained written comments on a draft of this report from the FEMA CIO. Generally, the FEMA CIO agreed with all of the report's findings and recommendations. We have incorporated the comments where appropriate and included a copy of the comments in their entirety at Exhibit D.

In his response, the FEMA CIO stated that FEMA is:

- Taking steps to ensure that entity-wide security program planning and management controls are in place to establish a framework and continuing cycle of activity to manage security risk;
- Working to ensure that the assignment of sensitive functions is legitimate, that the weaknesses that can lead to a control override in certain systems are mitigated, and that physical and electronic access to sensitive FEMA systems is secured and carefully monitored; and
- Continuing to develop applicable policies and procedures to ensure that certain duties are separated, as necessary and to monitor user roles and new user or access requests to prevent future segregation of duty conflicts.

OIG Response

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

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE WITHIN THE SCOPE OF THE FY 2007 DHS FINANCIAL STATEMENT AUDIT ENGAGEMENT – FEDERAL EMERGENCY MANAGEMENT AGENCY

Below is a description of significant FEMA's financial management systems and supporting IT infrastructure included in the scope of the FY 2007 DHS financial statement audit engagement.

Location of Testing: FEMA Headquarters in Washington, DC; the [redacted]; and the NFIP Bureau and Statistical Agent's facilities in [redacted].

Key Systems Subject to Testing:

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

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

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

Federal Emergency Management Agency
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement
Exhibit C

FY 2007 FEMA IT NFRs

Notice of Findings and Recommendation – Definition of Risk Ratings:

The Notice of Findings and Recommendations (NFR) were risk ranked as High, Medium, and Low based upon the potential impact that each weakness could have on the DHS component's information technology (IT) general control environment and the integrity of the financial data residing on the DHS component'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. 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. 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 Standards and reported in our *Independent Auditors' Report* on the DHS consolidated financial statements, dated November 15, 2007.

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
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement
Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-07-01	During our technical testing, patch management weaknesses were identified on [redacted] systems.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		X	High
FEMA-IT-07-02	During our technical testing, configuration management weaknesses were identified on [redacted], and key support servers.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		X	High
FEMA-IT-07-03	We determined that the Financial Services Bureau (FSB) 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, FSB is in the process of validating [redacted] access for users who responded to FSB's recertification request. In addition, FSB 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.	• Complete the recertification of [redacted] user access by removing the access of individuals who did not complete FEMA Form 20-24, [redacted] Access Control Form, and validating the existing [redacted] user access of individuals who completed FEMA Form 20-24. • Implement the OCFO Procedures for Granting Access to [redacted] by continuing to perform a review of all [redacted] access on a semi-annual basis including verifying the access privileges granted to federal employees and contractors.		X	High
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 SAN is not complete and therefore, the [redacted] facility does not have the capability of	FEMA should complete its efforts to implement the [redacted] "real-time" back-up facility as its alternate processing site and create redundant servers for the two [redacted] servers located at [redacted]		X	High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	functioning as the alternate processing site for [redacted] if a disaster were to occur.				
FEMA-IT-07-05	The [redacted] did not provide adequate documentation of the results to the accrediting authority and that the prior year weakness still exists.	Document the results of the [redacted] by providing a detailed listing for the vulnerabilities and/or corrective action for the vulnerabilities in the ATO as well as documenting them in an individual manner in the POA&M when the system is re-certified and accredited in FY 2008.		X	**Medium**
FEMA-IT-07-06	There is not formal, documented procedures are in place to require updates to the [redacted] system documentation as [redacted] functions are added, deleted, or modified.	Develop and implement procedures to require updates to [redacted] documentation as functions are added, deleted, or modified.		X	**Low**
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.	Perform a full-scale test of the [redacted] Contingency Plan once the [redacted] is operational as the alternate processing site for [redacted] [redacted] As a part of the full-scale contingency plan test, FEMA should include the critical IT components, such as key contingency personnel, backup servers at the alternate processing site, and use of backup tapes to bring up the system, in order to assess if they will operate as planned. Additionally, testing of the [redacted] Contingency Plan should be performed annually.		X	**Medium**
FEMA-IT-07-08	We determined that the FEMA COOP has not been updated to include the new listing of FEMA mission critical IT systems as outlined in the ITSD COOP Implementation Plan.	Update the FEMA COOP to clearly state and prioritize the listing of twenty-two (22) mission critical IT systems to be restored at its alternate processing site in the event of a disaster.		X	**Medium**
FEMA-IT-07-09	• We noted that FEMA has begun to standardize all user workstations to Microsoft Windows XP with Service Pack 2 installed, which would ensure	• Continue upgrading all FEMA domain level user's workstations operating system to Windows XP with Service Pack 2 installed and ensure that all [redacted] settings		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to Microsoft Windows XP 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.	are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver. • Ensure that FEMA users locked out of the system at the domain level after three consecutive failed login attempts remain locked for 20 minutes, per DHS IT *Security Program Sensitive System Handbook, 4300A*.			
FEMA-IT-07-10	We determined that FEMA has begun to standardize all user workstations to Microsoft Windows XP with Service Pack 2 installed, which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to Microsoft Windows XP 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]	Continue upgrading all FEMA domain level user workstation operating systems to Windows XP with Service Pack 2 installed and ensure that all [redacted] settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver.		X	**Medium**
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 IT Security Program Sensitive System	• Configure the [redacted] application to require passwords to not be reused until eight (8) iterations have passed to be in compliance with DHS IT Security Program, 4300A		X	**Medium**

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Handbook, 4300A.	Password Policy.			
FEMA-IT-07-12	• 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. 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.	• Complete implementation of procedures regarding the periodic review of [redacted] access lists, including the frequency of the review. Furthermore, FEMA should complete the review of [redacted] user access for FY 2007 by taking all responses received for users and updating [redacted] user access accordingly. • Continue to develop the automated process around granting, removing and validating [redacted] user access and implement by March 2008, per the FY 2006 FEMA IT Financial Audit Remediation Plan.		X	Medium
FEMA-IT-07-13	• We determined that the FSB 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. Currently, FSB is in the process of validating [redacted] access for the users who responded to FSB's recertification request and locking out the [redacted] users who did not respond. We determined	• Complete the recertification of [redacted] user access by removing the access of individuals who did not complete FEMA Form 20-24, [redacted] Access Control Form, and validating the existing [redacted] user access of individuals who completed FEMA Form 20-24. • Implement the OCFO Procedures for Granting Access to [redacted] by continuing to perform a review of all [redacted] access on a semi-annual basis including verifying the access privileges granted to federal employees and contractors.		X	High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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.	• Complete implementation of procedures regarding the periodic review of [redacted] access lists, including the frequency of the review. Furthermore, FEMA should complete the review of [redacted] user access for FY 2007 by taking all responses received for users and updating [redacted] user access accordingly. • Continue to develop the automated process around granting, removing and validating [redacted] user access and implement by March 2008, per the FY 2006 FEMA IT Financial Audit Remediation Plan. • Per FEMA Instruction 1540.3, perform a review of authorized accounts on a semi-annual basis and remove terminated employees' access to all FEMA systems.			
FEMA-IT-07-14	• We determined that IT Operations has created backup procedures entitled, *Backup Media Protection and Control*,	• Implement the *Backup Media Protection and Control* by performing the [redacted] backups on a regular basis. When performing		X	High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	for [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] 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] in June 2007. Therefore, the risk was present for a majority of the fiscal year.	[redacted] backups, FEMA should: • Maintain a documented backup inventory for [redacted], • Rotate [redacted] backups off-site to the [redacted] on a regular basis, • Log the deposit and withdrawal of [redacted] backup tapes is maintained, and • Ensure that logs are maintained per the stated retention time period. • Complete its efforts to implement the [redacted] "real-time" back-up facility as its alternate processing site. Ensure that redundant servers are created at the [redacted] for the [redacted] and [redacted] servers located [redacted].			
FEMA-IT-07-15	• We determined that FEMA created the [redacted] Configuration Management Plan, Version 0.1, 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 Sensitive Systems Policy Directive 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.	• Finalize the [redacted] Configuration Management Plan to be in compliance with DHS IT Security Program Sensitive System Handbook, 4300A. • Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B. • Implement the *Database Administration Access Procedures* and [redacted] patch management procedures.		X	High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• We noted that procedures over restricting access to [redacted] system software entitled, *Database Administration Access 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 Sensitive Systems Policy Directive 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.	• Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B. • Develop and implement specific procedures for restricting access to [redacted] system software, and promulgate it to all needed personnel, to be in compliance with DHS IT Security Program Sensitive System Handbook, 4300A.		X	**Medium**
FEMA-IT-07-17	• We determined that FEMA created a System Change Request Standard Operating Procedures (SOP) for [redacted]. However, the System Change Request SOP was approved by the OCFO on June 29, 2007. Furthermore, we noted the evidence that the "[redacted]" account was locked within the UNIX environment on July 24, 2007. Therefore, we noted that the risk was present for a majority of the fiscal year.	Implement the System Change Request SOP by keeping the "[redacted]" account locked at all times, except when a change needs to be deployed in the [redacted] production environment, and by monitoring the [redacted]" directory and sub-directories to detect updates.		X	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-07-18	• FEMA created the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 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].	• Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B. • Develop and implement specific procedures for the review of suspicious system software activity and access controls for [redacted], and promulgate it to all needed personnel.		X	Medium
FEMA-IT-07-19	• FEMA created the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 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].	• Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B, • Develop and implement specific procedures to monitor sensitive access and system software utilities for [redacted], and promulgate it to all needed personnel, and • Develop and implement specific procedures to review suspicious system software and access activities for [redacted], and promulgate it to all needed personnel.		X	Medium
FEMA-IT-07-20	FEMA has adopted the DHS SDLC Version 0.5.1 for [redacted]. This policy establishes required practices for managing DHS IT	Implement the DHS SDLC for [redacted] program development when DHS finalizes the document. Additionally, FEMA should ensure that the SDLC		X	High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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.	methodology is promulgated to all personnel involved in the design, development, and implementation process.			
FEMA-IT-07-21	FEMA has adopted the DHS SDLC Version 0.5.1 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.	Implement the DHS SDLC for [redacted] program development when DHS finalizes the document. Additionally, FEMA should ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process.		X	High
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] Oracle Database effective as of June 2007.	FEMA should complete its efforts to implement the [redacted] "real-time" back-up facility as its alternate processing site. Ensure that redundant servers are created at the [redacted] [redacted] for the [redacted] servers located at the [redacted]	X		High
FEMA-IT-07-23	FEMA lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.	• Develop and implement procedures to periodically test the [redacted] backups in compliance with DHS IT Security Program Sensitive System Handbook 4300A. • Periodically test [redacted] backups at least annually in compliance with DHS IT Security Program Sensitive System Handbook 4300A.	X		High

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-07-24	FEMA lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.	• Develop and implement procedures to periodically test the [redacted] backups in compliance with DHS IT Security Program Sensitive System Handbook 4300A. • Periodically test [redacted] backups at least annually in compliance with DHS IT Security Program Sensitive System Handbook 4300A.	X		**High**
FEMA-IT-07-25	We noted that the [redacted] contingency plan has not been tested on an annual basis, per DHS Sensitive Systems Policy Directive 4300A.	Perform an annual test of the [redacted] Contingency Plan, which covers all critical phases of the plan.	X		**High**
FEMA-IT-07-26	During our review of user access rights for the approval of [redacted] system change requests, we noted that excessive access rights existed. Specifically, we determined that three (3) people were authorized to approve [redacted] system change requests, however, one (1) individual was transferred to another DHS agency. Therefore, this person's job responsibilities no longer required this access nor is this individual a current FEMA employee. Upon notification of this issue, FEMA took corrective action and removed the individual's access rights.	Develop a process to review user access for the approval of [redacted] system change requests to determine if access is needed.	X		**Medium**
FEMA-IT-07-27	We noted that testing documentation for [redacted] application level changes are not consistently documented or performed timely.	• Ensure all [redacted] application level changes are tested in a timely fashion. • Ensure all test data and transactions are appropriately documented and maintained with the respective system change request within the system, per the [redacted]	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		Configuration Management Plan.			
FEMA-IT-07-28	Per *DHS Sensitive Systems Policy Directive 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.	• Ensure all [redacted] application level changes are tested. • Ensure all test data and transactions are appropriately documented and maintained with the respective system change request within the system.	X		**Medium**
FEMA-IT-07-29	We noted that the TRC 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 TRC approval.	Ensure all [redacted] application level emergency changes obtain TRC approval prior to being implemented into the production environment.	X		**Medium**
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] 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.	Implement a solution to limit the excessive access to make offline changes to the general ledger account tables. Access rights should be periodically reevaluated and limited to people who have a business need.		X	**High**
FEMA-IT-07-31	• [redacted] does not timeout after a period of inactivity. Additionally, we determined that all NFIP workstations use a password protected screensaver after fifteen (15) minutes of inactivity, which is not in compliance with DHS	• Configure the domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with DHS IT Security Program Sensitive System Handbook, 4300A. • Develop and implement policies and		X	**Medium**

Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	4300A. • [redacted] access is not reviewed on a periodic basis to determine if access is valid and commensurate with job responsibilities.	procedures regarding periodic review of [redacted] access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege.			
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.	• Document the change management procedures for [redacted] • Develop and implement change management procedures over system software changes and establish documented approvals prior to installing or upgrading system software.		X	**Medium**
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.	Ensure that Computer Sciences Corporation (CSC) develop and implement procedures for reviewing [redacted] logs on a monthly basis. The procedures should include investigation of suspicious activity or suspected violations and reporting findings to appropriate officials.		X	**Low**
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 OSR forms or documented approvals.	Ensure that CSC document and implement change management procedures requiring approvals prior to implementing changes in the production environment.		X	**Medium**

Exhibit C

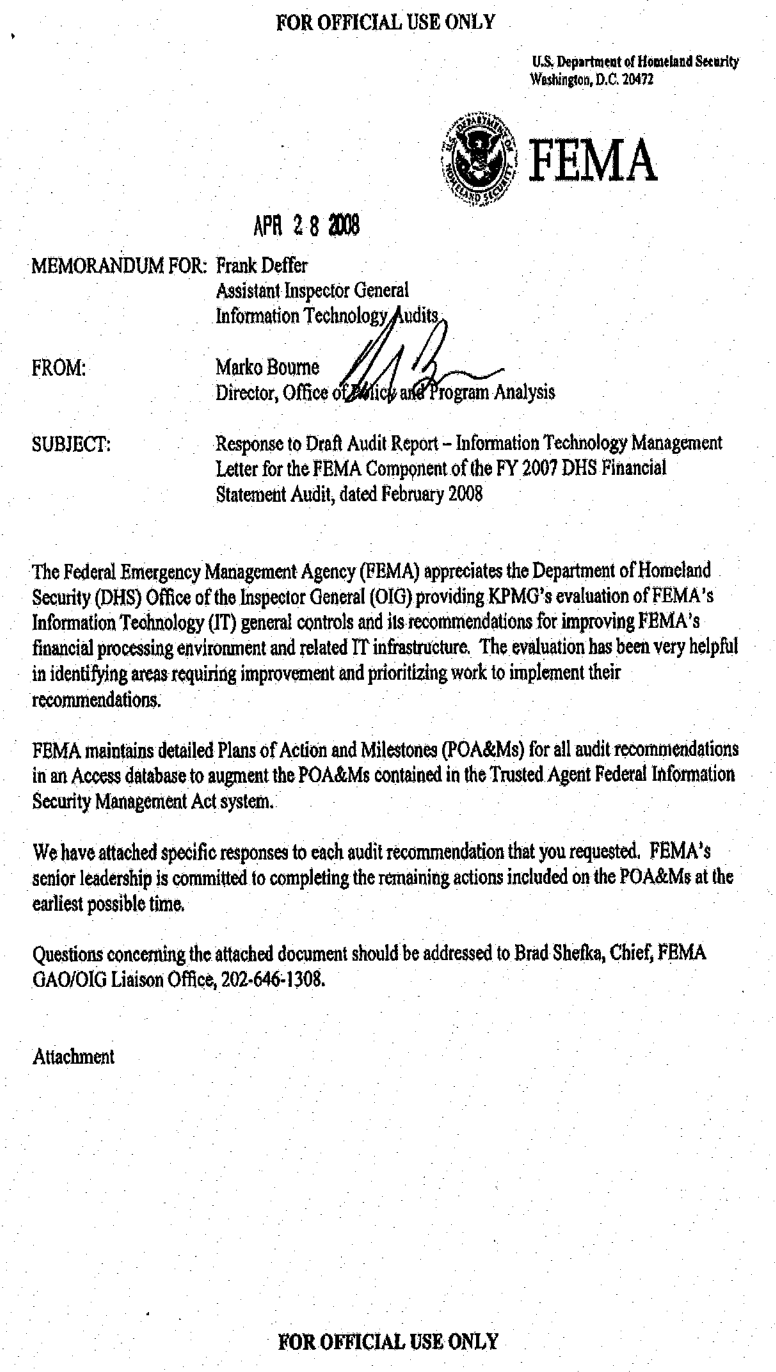
NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-07-35	A system programmer [redacted]) had write access to the [redacted] datasets of the [redacted] production member. NFIP removed the system programmer's access shortly after this finding was identified.	Ensure that CSC develop and implement procedures to perform a periodic review of access to mainframe production datasets to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.		X	**Medium**
FEMA-IT-07-36	Access to the LAE 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.	Ensure that CSC restricts access to the LAE excel files to the Actuary and Finance Director in order to achieve the principle of least privilege.		X	**Medium**
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.	• Remove excessive access to the [redacted] application software and support files. • Develop and implement procedures to perform a periodic review of access to [redacted] application software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.	X		**Medium**
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.	• Identify and document incompatible duties, and system roles and responsibilities within [redacted]. • Develop and implement policies and procedures segregating incompatible duties within [redacted], to be in compliance with DHS IT Security Program Sensitive System Handbook, 4300A. • Identify and implement capabilities within [redacted] that enforce segregation of incompatible duties.		X	**Medium**

Federal Emergency Management Agency
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement
Exhibit C

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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] alternate processing facility; and • [redacted] critical data files are not documented.	• Perform a test the [redacted] Contingency Plan, covering all critical phases of the plan on an annual basis. • Perform a test of the system fail-over capability at the alternate processing site. • Revise the Disaster Recovery and COOP to incorporate the [redacted] alternate processing facility and the [redacted] critical data files.	X		**Medium**
FEMA-IT-07-40	The Rules of Behavior forms are not consistently signed prior to users gaining access to the [redacted]. Specifically, we determined that three (3) out of a sample of twelve (12) new [redacted] [redacted] users did not sign the Rules of Behavior prior to obtaining [redacted] [redacted]	Ensure that CSC require all employees and contractors acknowledge and sign a Rules of Behavior prior to being granted access to the [redacted] [redacted]	X		**Medium**
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].	Ensure that CSC develop and implement procedures to perform a periodic review of access to [redacted] production datasets to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.		X	**Medium**
FEMA-IT-07-42	We determined that periodic review policies and procedures have not been developed for access to the [redacted] room. As a result, we noted that there are two (2)	Ensure that CSC develops and implements policies and procedures to periodically review physical access listings over the [redacted] Room to determine if access is still required or if access		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	employees with excessive access to the [redacted] room.	levels commensurate with users' job responsibilities.			
FEMA-IT-07-43	The [redacted] has been configured to permit users to reuse prior passwords after five (5) iterations which is not in compliance with the DHS IT Security Program Sensitive System Handbook, 4300A.	Ensure that CSC configures the [redacted] to require passwords to not be reused until eight (8) iterations have passed to be in compliance with DHS IT Security Program, 4300A Password Policy.	X		**Medium**
FEMA-IT-07-44	We noted that proactive vulnerability scanning is not performed over [redacted] backend database or the [redacted].	Ensure that CSC perform vulnerability scans over the [redacted] backend database or the [redacted] on an annual basis.	X		**Medium**

Federal Emergency Management Agency
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement
Exhibit D



FOR OFFICIAL USE ONLY

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

FEMA

APR 28 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Marko Bourne
Director, Office of Policy and Program Analysis

SUBJECT: Response to Draft Audit Report – Information Technology Management Letter for the FEMA Component of the FY 2007 DHS Financial Statement Audit, dated February 2008

The Federal Emergency Management Agency (FEMA) appreciates the Department of Homeland Security (DHS) Office of the Inspector General (OIG) providing KPMG's evaluation of FEMA's Information Technology (IT) general controls and its 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 maintains detailed Plans of Action and Milestones (POA&Ms) for all audit recommendations in an Access database to augment the POA&Ms contained in the Trusted Agent Federal Information Security Management Act system.

We have attached specific responses to each audit recommendation that you requested. FEMA's senior leadership is committed to completing the remaining actions included on the POA&Ms at the earliest possible time.

Questions concerning the attached document should be addressed to Brad Shefka, Chief, FEMA GAO/OIG Liaison Office, 202-646-1308.

Attachment

FOR OFFICIAL USE ONLY

Attachment

Federal Emergency Management Agency
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement Exhibit A

RESPONSES TO INFORMATION TECHNOLOGY GENERAL CONTROL RECOMMENDATIONS

A. Entity-wide Security Program Planning and Management

Recommendation #1. *Document the results of the* [redacted] *by providing a detailed listing for the vulnerabilities and/or corrective action for the vulnerabilities in the authority to operate (ATO) and documenting them in an individual manner in the Plan of Actions and Milestones (POA&M) when the system is re-certified and accredited in FY 2008.*

FEMA concurs that a new, full Certification and Accreditation (C&A) of [redacted] is due to meet the 3 year C&A cycle and to address major changes to [redacted]. [redacted] changes include establishing a Continuity of Operations Plan (COOP) site, failover capability, and a new production server and version of Oracle. FEMA completed the C&A on March 31, 2008.

B. Access Controls

Recommendation #1. *Implement the corrective actions for each of the weaknesses identified during the vulnerability assessment testing as listed in the specific NFR.*

FEMA concurs with this recommendation. FEMA has developed a POA&M for all of the recommendations and monitors the progress of the POA&Ms through weekly meetings with the responsible Branch Chiefs. Additionally FEMA issued a "Penetration and Vulnerability Reporting" Standard Operating Procedure (SOP) on February 27, 2008. Procedures include monthly scanning and the prioritization of corrective actions to mitigate high risk vulnerabilities. FEMA implemented the corrective actions in 2nd quarter FY08.

Recommendation #2. *Complete the recertification of* [redacted] *user access by removing the access of individuals who did not complete FEMA Form 20-24, IFMIS Access Control Form, and validate the existing* [redacted] *user access of individuals who completed FEMA Form 20-24.*

FEMA concurs with this recommendation. A recertification of [redacted] users was conducted and unauthorized users were removed as of September 2007. No further remediation activities will follow for this recommendation.

Recommendation #3. *Implement the Office of Chief Financial Officer (OCFO) Procedures for Granting Access to* [redacted] *by continuing to perform a review of all* [redacted] *access on a semi-annual basis including verifying the access privileges granted to federal employees and contractors.*

FEMA concurs with this recommendation. The FEMA OCFO distributed a memorandum commencing another [redacted] access review in early January with the goal of terminating accounts by March 14, 2008. A semi-annual process has been put in place with procedural applicable guidance to assure the reviews occur. FEMA implemented the OCFO procedures in 2nd quarter FY08.

Recommendation #4. *Complete implementation of procedures regarding the periodic review of* [redacted] *access lists, including a review of accounts on a semi-annual basis and removal of terminated employees' access to all FEMA systems.*

FEMA concurs with this recommendation. FEMA completed removing account roles from employees according to the "least privilege" principle in January 2008. A semi-automated, semi-annual process to validate access to [redacted] and remove unnecessary account roles is being developed, along with procedural guidance addressing the semi-annual review. FEMA is changing its procedures for dropping locked accounts of terminated employees from 90 days to 45 days in accordance with the DHS Sensitive Systems Policy Directive 4300A. FEMA completed the implementation of new procedures on March 31, 2008.

Recommendation #5. *Continue development of the automated process of granting, removing, and validating* [redacted] *user access and implement by March 2008, per the FY 2006 FEMA IT Financial Audit Remediation Plan.*

FEMA concurs with this recommendation. A semi-automated, semi-annual process to validate access to [redacted] and remove unnecessary account roles is being developed, along with procedural guidance addressing the semi-annual review. FEMA completed the implementation of new procedures on March 31, 2008.

Recommendation #6. *Continue upgrade of all FEMA domain level user's workstations operating system to Windows XP with Service Pack 2 installed and ensure that all* [redacted] *settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver.*

FEMA concurs with this recommendation. FEMA distributed a memorandum directing the upgrade and lock out of Windows 2000 machines and setting Windows XP Service Pack 2 as the standard in February 2008. Regional IT Branch Chiefs are coordinating the upgrade of machines. The inactivity threshold in [redacted] is set to correspond to DHS 4300A and is correct. FEMA will block FEMA domain access from legacy systems on March 31, 2008. Resolution of Recommendation #6 was completed March 31, 2008.

Recommendation #7. *Ensure that FEMA users locked out of the system at the domain level after three consecutive failed login attempts remain locked for 20 minutes, per DHS IT Security Program Sensitive System Handbook, 4300A.*

FEMA concurs with this recommendation. The inactivity threshold in [redacted] is set to correspond to DHS 4300A requirements. No further remediation activities are planned.

Recommendation #8. *Configure the [redacted] application to require passwords not be reused until eight (8) iterations have passed to be in compliance with DHS IT Security Program, 4300A.*

FEMA concurs with this recommendation. This action was completed. The [redacted] application now requires passwords to go through 8 iterations before being reused in accordance with DHS IT Security Program, 4300A. No further remediation activities are planned.

Recommendation #9. *Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B.*

FEMA concurs with this recommendation. The Supplemental Security Policy was completed, circulated for review, and was awaiting approval and sign off. Recently, a new Chief Information Security Officer (CISO) was appointed at FEMA. The CISO reviewed the policy and directed some changes to the document. The Policy is currently being vetted for final approval.

Recommendation #10. *Develop and implement specific procedures for restricting access to [redacted] system software, and promulgate it to all needed personnel, to be in compliance with DHS IT Security Program Sensitive System Handbook, 4300A.*

FEMA concurs with this recommendation. Procedures were developed and implemented on 31 July 2007. Testing of these procedures will continue to ensure the control is effective. No further remediation is planned for this recommendation.

Recommendation #11. *Develop and implement policies and procedures to periodically review physical access listings over the [redacted] room to determine if access is still required or if access levels are commensurate with users' job responsibilities.*

FEMA concurs with this recommendation. A policy and procedure was developed for conducting quarterly reviews of the card key access database. Computer Sciences Corporation (CSC) Security has been performing access reviews since the late fall 2007. Procedures are documented in the [redacted] Administration Manual 2007. No further remediation activities are planned for this recommendation.

Recommendation #12. *Configure the [redacted] domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with DHS IT*

Security Program Sensitive System Handbook, 4300A.

FEMA concurs with this recommendation. FEMA decreased the password protected screensaver to five (5) minutes in October 2007. No further remediation activities are planned for this recommendation.

Recommendation #13. *Develop and implement policies and procedures regarding periodic review of* [redacted] *access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege.*

FEMA concurs with this recommendation. In the fall of 2007, FEMA instituted the [redacted] Procedures 2007. This stipulates the policy and procedural requirement for a quarterly review of [redacted] logical user access based on least privilege. No further remediation activities are planned for this recommendation.

Recommendation #14. *Restrict access to the Louisiana Association of Educators (LAE) Excel files to the Actuary and Finance Director in order to achieve the principle of least privilege.*

FEMA concurs with this recommendation. Access to the LAE Excel files was restricted to 3 people, to include the Project Director. Policy and procedures regarding access is included in the [redacted] Manual 2007. No further remediation activities are planned for this recommendation.

Recommendation #15. *Ensure that the* [redacted] *is configured to require passwords to not be reused until eight (8) iterations have passed in order to be in compliance with DHS IT Security Program, 4300A.*

FEMA concurs with this recommendation. Parameters on the [redacted] were increased to require passwords go through eight (8) iterations from five (5) in the fall 2007. This is documented in the [redacted] Manual 2007. No further remediation activities are planned for this recommendation.

Recommendation #16. *Perform vulnerability scans over the* [redacted] *backend database and the* [redacted] *on an annual basis.*

FEMA concurs with this recommendation. [redacted] Network Security Scanner was recently acquired to implement scanning by March 31, 2008. Policy is included in the NFIP Bureau Statistical Agent (BSA) [redacted] Administrator Manual that requires weekly [redacted] scans that will include [redacted]. Recommendation #16 will be implemented by June 30, 2008.

C. Application Software Development and Change Control

Recommendation #1. *Finalize and implement the* [redacted] *Configuration Management Plan to be in compliance with DHS IT Security Program Sensitive System Handbook, 4300A.*

FEMA concurs with this recommendation. The [redacted] Configuration Management Plan was finalized and implemented on July 31, 2007 and submitted to the KPMG auditor. The implemented plan is in compliance with DHS 4300A. An update was completed on March 17, 2008 to incorporate a new procedure for approving System Change Requests. Testing to verify effective implementation was completed March 31, 2008.

Recommendation #2. *Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B.*

FEMA concurs with this recommendation. The Supplemental Security Policy was completed, circulated for review, and was awaiting approval and sign off. Recently, a new CISO was appointed at FEMA. The CISO reviewed the policy and directed some changes to the document. The Policy is currently being vetted for final approval.

Recommendation #3. *Implement the Database Administration Access procedures and* [redacted] *patch management procedures.*

FEMA concurs with this recommendation. The procedures were implemented, with testing, to ensure procedures are effectively implemented in 2nd quarter FY08.

Recommendation #4. *Implement the DHS System Development Life Cycle (SDLC) for* [redacted] *program development when DHS finalizes the document. Additionally, FEMA should ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process.*

FEMA concurs with this recommendation. The DHS Systems Life Cycle (SLC) is the official guidance being followed at FEMA even though it is in draft form. The document is promulgated for all FEMA personnel's use via a website on the intranet. FEMA is using this DHS SLC for both [redacted] Operational phase activities. FEMA has documented that use in the respective System Security Plans, yearly OMB A-11 Exhibit 300s, and C&A packages. FEMA will continue using the DHS SLC draft until DHS completes a finalized version. No further remediation activities are planned for this recommendation.

Exhibit D

Recommendation #5. *Ensure that the NFIP Bureau and Statistical Agent documents and implements change management procedures requiring approvals prior to implementing changes in the* [redacted] *production environment.*

FEMA concurs with this recommendation. FEMA's [redacted] System Change Control and System Change Control procedures are documented. FEMA has required approval of all changes since the fall 2007. No further remediation activities are planned for this recommendation.

Recommendation #6. *Develop a process to periodically review user access for the approval of* [redacted] *system change requests to determine if access is needed.*

FEMA concurs with this recommendation. The [redacted] Configuration Management (CM) Plan was updated in January 2008 to include periodically reviewing those authorized to approve change requests. Testing compliance of the plan was completed March 31, 2008.

Recommendation #7. *Ensure all* [redacted] *application level changes are tested in a timely manner.*

FEMA concurs with this recommendation. The [redacted] CM Plan was developed and implemented by July 31, 2007. Updates required to the [redacted] CM Plan were recently identified and are being completed. The [redacted] CM Plan was developed and documented in November 2007. Testing of this plan was completed March 31, 2008.

Recommendation #8. *Ensure all test data and transactions are appropriately documented and maintained with the respective system change request within the system.*

FEMA concurs with this recommendation. The CM Directive is currently in the final vetting process. Upon issuance, implementation of this item will be tested.

Recommendation #9. *Ensure all* [redacted] *application level emergency changes obtain TRC approval prior to being implemented into the production environment.*

FEMA concurs with this recommendation. Updates were made to the [redacted] CM Plan to ensure the approval of [redacted] emergency System Change Requests (SCRs) before implementation. Testing of this plan was completed March 31, 2008.

Recommendation #10. *Remove excessive access to the* [redacted] *application software and support files.*

FEMA concurs with this recommendation. The Bureau of Finance and Statistical Control staff has reviewed and accepts the current levels of access. The acceptance of the levels of access for financial management personnel was signed March 31, 2008.

Recommendation #11. *Develop and implement procedures to perform a periodic review of access to* [redacted] *application software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.*

FEMA concurs with this recommendation. Procedures for controlling and annually reviewing [redacted] access will be included in the [redacted] Desktop Procedures 2008 (4.4). Recommendation #11 is scheduled to be completed in the fall 2008.

D. System Software

Recommendation #1. *Implement the System Change Request Standard Operating Procedures by keeping the* [redacted]*" account locked at all times, except when a change needs to be deployed in the* [redacted] *production environment, and by monitoring the "*[redacted]*" directory and sub-directories to detect updates.*

FEMA concurs with this recommendation. A Standard Operating Procedure (SOP) was provided to the KPMG auditor on June 29, 2007 addressing this recommendation. This SOP was implemented that day and is still in effect. Testing to verify compliance with the SOP was completed 2nd quarter FY08.

Recommendation #2. *Finalize and implement the Supplemental Security Policy to the DHS Sensitive Systems Policy Directive 4300A and 4300B.*

FEMA concurs with this recommendation. The final Supplemental Security Policy was implemented 2nd quarter FY08.

Recommendation #3. *Develop and implement specific procedures for the review of suspicious system software activity and access controls for* [redacted]*, and promulgate it to all needed personnel.*

FEMA concurs with this recommendation. An [redacted] Standard Operating Procedure (SOP) was developed and provided to the KPMG auditor on June 29, 2007 addressing this recommendation. It was circulated to appropriate personnel and implemented. This control was tested March 31, 2008. [redacted] completed an SOP that was implemented on February 27, 2008.

Recommendation #4. *Develop and implement specific procedures to monitor sensitive access and system software utilities for* [redacted]*, and promulgate it to all needed personnel.*

Exhibit D

FEMA concurs with this recommendation. [redacted] completed an SOP that was implemented on February 27, 2008 to address this recommendation. No further remediation activities are planned for this recommendation.

Recommendation #5. *Document the change management procedures for the* [redacted] *application.*

FEMA concurs with this recommendation. [redacted] System Change Control and System Change Control procedures are documented. They include the requirement for approval of changes. This has been in effect since the fall of 2007. No further remediation activities are planned for this recommendation.

Recommendation #6. *Develop and implement change management procedures for* [redacted] *system software changes and establish documented approvals prior to installing or upgrading system software.*

FEMA concurs with this recommendation. [redacted] System Change Control and System Change Control procedures are documented. They include the requirement for approval of changes. This has been in effect since the fall of 2007. No further remediation activities are planned for this recommendation.

Recommendation #7. *Ensure that the NFIP Bureau and Statistical Agent develops and implements procedures to perform a periodic review of access to* [redacted] *production datasets to determine whether access is valid, consistent with job responsibilities, and conformed to the least privilege principle.*

FEMA concurs with this recommendation. A review will be performed of the procedures for validating dataset role access in June 2008 as part of the transition to NextGen technologies. Evidence will be available by July 31, 2008.

E. Service Continuity

Recommendation #1. *Complete efforts to implement the* [redacted] *data center's "real-time" back-up facility as its alternate processing site and create redundant servers for the* [redacted] *servers located at* [redacted].

FEMA concurs with this recommendation. FEMA is submitting a waiver request for the [redacted] COOP site with the plan to move to a DHS data center. [redacted] is building a COOP site in [redacted]. FEMA's plan to complete the COOP site, with real time replication of the production system at [redacted], was completed 2nd quarter FY08.

Recommendation #2. *Implement the new developed Backup Media Protection and Control procedures by performing the* [redacted] *backups on a regular basis. When performing* [redacted] *backups, FEMA should:*

- *Maintain a documented backup inventory for* [redacted].
- *Rotate* [redacted] *backups off-site to the* [redacted] *on a regular basis.*
- *Log the deposit and withdrawal of* [redacted] *backup tapes.*
- *Ensure that logs are maintained per the stated retention time period.*
- *Develop and implement procedures to test the* [redacted] *backups at least annually in compliance with DHS IT "Security Program Sensitive System Handbook, 4300A".*

FEMA concurs with this recommendation. FEMA sent procedures and documentation on backups and controls for both the [redacted] systems to the OIG Auditor on June 29, 2007. Both [redacted] continue these backup practices, which are listed above. Compliance with the procedures is scheduled for testing prior to March 31, 2008. Backups are tested at least annually for both systems. [redacted] testing documentation was sent to the KPMG Auditor by July 2007. [redacted] completed a SOP for testing backups and documenting recovery from tape in 2nd quarter FY08.

Recommendation #3. *Perform an annual test of the* [redacted] *contingency plan, which covers all critical phases of the plan.*

FEMA concurs with this recommendation [redacted] requested a waiver for the COOP site and a full scale contingency plan test. This is based on FEMA's plan to move to a DHS data center within a few years.

Recommendation #4. *Perform a full-scale test of the* [redacted] *contingency plan once the* [redacted] *data center is operational as the alternate processing site for* [redacted]. *As a part of the full-scale contingency plan test, FEMA should include the critical IT components, such as key contingency personnel, backup servers at the alternate processing site, and use of backup-tapes to bring up the system, in order to assess if they will operate as planned. Additionally, a test of the* [redacted] *contingency plan should be performed annually.*

FEMA concurs with this recommendation. FEMA completed testing and documenting the results of the [redacted] contingency plan in March 2008. Annual testing of the [redacted] contingency plan has been scheduled.

Recommendation #5. *Update the COOP to clearly state and prioritize the listing of 22 mission critical IT systems to be restored at its alternate processing site in the event of a disaster.*

FEMA concurs with this recommendation. The FEMA COOP Plan was updated 31 March 2008 to include the 22 mission critical IT systems.

Recommendation #6. *Perform a test of the* [redacted] *contingency plan, covering all critical phases of the plan on an annual basis.*

FEMA concurs with this recommendation. Under the new Bureau and Statistical Agent (BSA) and NFIP IT contracts new contingency plans will be developed to ensure that [redacted] is fully planned and tested for contingency operations. Expected completion date is June 30, 2008.

Recommendation #7. *Perform a test of the system fail-over capability at the alternate processing site for* [redacted].

FEMA concurs with this recommendation. Under the new Bureau and Statistical Agent (BSA) and NFIP IT contracts a COOP site will be developed to ensure that [redacted] is fully planned and tested for contingency operations. Expected completion date is June 30, 2008.

Recommendation #8. *Revise the Disaster Recovery and COOP to incorporate the* [redacted] *alternate processing facility and the* [redacted] *critical data files.*

FEMA concurs with this recommendation. Under the new BSA and NFIP IT Contracts new Disaster Recovery and COOP plans will be developed to ensure that [redacted] is fully planned and tested for contingency operations. Expected completion date is June 30, 2008.

Recommendation #9. *Ensure that all employees and contractors acknowledge and sign Rules of Behavior (ROB) prior to being granted access to the* [redacted].

FEMA concurs with this recommendation. A new [redacted] with corresponding security documentation is under development for the Bureau and NFIP IT operations that will ensure all users sign the ROB prior to gaining authorized access. Expected completion date is June 1, 2008.

F. Segregation of Duties

Recommendation #1. *Identify and document incompatible duties and system roles and responsibilities within* [redacted].

FEMA concurs with this recommendation. Implementation of this recommendation is scheduled for completion by June 30, 2008.

Recommendation #2. *Develop and implement policies and procedures segregating incompatible duties within* [redacted], *to be in compliance with DHS Information Technology Security Program Sensitive System Handbook, 4300A.*

FEMA concurs with this recommendation. Implementation of this recommendation is scheduled for completion by June 30, 2008.

Recommendation #3. *Identify and implement capabilities within* [redacted] *that enforce segregation of incompatible duties.*

FEMA concurs with this recommendation. Implementation of this recommendation is scheduled for completion by June 30, 2008.

Exhibit E

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
Chief Information Officer
Chief Financial Officer
Chief Financial Officer, FEMA
Chief Information Officer, FEMA
Chief Information Security Officer
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Office of Legislative Affairs
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, 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.