

DEPARTMENT OF HOMELAND SECURITY

# Office of Inspector General

## **Management Letter for FEMA's Fiscal Year 2002 Financial Statement Audit**



Office of Audits

OIG-04-03

December 2003

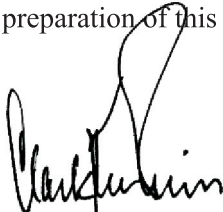


## Preface

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, investigative, and special reports prepared by the OIG periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. The independent public accounting firm KPMG LLP performed the audit. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein, if any, have been developed on the basis of the best knowledge available to KPMG and the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.



Clark Kent Ervin  
Acting Inspector General





# Contents

---

Preface	
Table of Contents .....	i
Executive Summary .....	1
Appendix A: FY02 Comments and Recommendations .....	3
Appendix B: Summary status of comments reported in the FY 2001 Management Letter .....	11
Appendix C: Analysis of Management Comments.....	15
Appendix D: Management Comments-FAMD.....	17
Appendix E: Management Comments-ITSD.....	18
Appendix F: Management Comments-OGFC .....	19
Appendix G: Management Comments-Region II.....	23
Appendix H: Management Comments-Region IX .....	26
Appendix I: OIG contributors to this report .....	29
Appendix J: Report Distribution.....	30





2001 M Street NW  
Washington, DC 20036

January 24, 2003

Office of Inspector General, Federal Emergency Management Agency  
and Acting Chief Financial Officer, Federal Emergency Management Agency:

We have audited the consolidated financial statements of the Federal Emergency Management Agency (FEMA) for the year ended September 30, 2002, and have issued our report thereon dated January 24, 2003. In planning and performing our audit of the consolidated financial statements of FEMA, we considered internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing an opinion on the consolidated financial statements. An audit does not include examining the effectiveness of internal control over financial reporting and does not provide assurance on internal control over financial reporting. We have not considered internal control over financial reporting since the date of our report.

During our audit, we noted certain matters involving internal control over financial reporting and other operational matters that are presented for your consideration in Appendix A. Appendix B presents the status of matters reported in our management letter dated February 6, 2002. These comments and recommendations are intended to improve FEMA's internal control or result in other operating efficiencies. We discussed all these findings and recommendations with management, and their written responses, as well as our analysis of their written responses, are included as appendices to this letter.

The comments and recommendations outlined in Appendix A and Appendix B are in addition to the following reportable conditions in internal control over financial reporting included in our separate report on the consolidated financial statements dated January 24, 2003, the first six of which we considered to be material weaknesses:

- Information security controls for FEMA's financial systems environment
- FEMA's financial system functionality
- FEMA's financial reporting process
- FEMA's real and personal property accounting systems and processes
- FEMA's account reconciliation processes
- FEMA's accounts receivable processes
- FEMA's Cerro Grande estimation processes

These matters were considered in determining the nature, timing, and extent of the audit tests applied in our audit of the FEMA consolidated financial statements.

Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statements, and therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of FEMA's organization gained during our work to make



KPMG LLP KPMG LLP, a U.S. limited liability partnership, is  
a member of KPMG International, a Swiss association.



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 solely for the information and use of FEMA's management, FEMA's Office of Inspector General (OIG), the U.S. Office of Management and Budget (OMB), and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP



**1. Human Resources Division (HRD)**

Based on our review of 32 items related to the Federal Employees' Group Life Insurance (FEGLI) Program, we noted three instances in which the life insurance cost deducted from the employee's paycheck was not supported by a SF-2817, *Life Insurance Election*. All eligible employees are covered unless they decline coverage in writing by completing the SF-2817. The SF-2817 also documents the amount of coverage chosen. In two of the instances, the SF-2817 showed that the employee had elected coverage for which the cost did not match the cost deduction from the employee's paycheck. In the third instance, no SF-2817 existed in the employee's personnel file; therefore, the life insurance cost deducted from the employee's paycheck could not be verified. FEMA was unable to provide current SF-2817 forms or other supporting documentation to support the life insurance costs deducted from these three employee paychecks.

As a result of this issue, the employees' withholdings, federal government contributions to the program, and payment of program benefits could be incorrect.

The Office of Personnel Management (OPM) has overall authority and responsibility for the FEGLI program, and in turn, OPM has delegated authority to the individual agencies to accomplish the following: 1) determine the coverage eligibility of participants; 2) collect and timely remit participant withholdings and agency contributions in a timely manner; and 3) maintain individual participant records to ensure proper control of the program. In addition, the *Standards for Internal Control in the Federal Government* issued by the General Accounting Office (GAO) requires that the documentation that supports entity transactions and significant events should be readily available for examination.

- 1.1 We recommend that HRD perform periodic checks of personnel files to ensure that the most current documentation is maintained to support the employees' FEGLI election and other benefit elections.

**2. Cerro Grande Claims Administration**

The Office of Cerro Grande Fire Claims (OCGFC) Payment Approval System (PAS) serves as a workflow manager and payment approval processing tool for submitted fire claims. PAS allows claims reviewers to review claim information and authorizing officials to approve claim payments. PAS was initially designed as a personal computer (PC) based system. However, as the volume of claims increased, it was migrated to a network-based system. PAS was implemented at OCGFC in November 2000 by a contractor, who continues to work with OCGFC to support the system.

There are three security access levels for PAS, as follows:

- Network level - requires a unique user ID and password to gain access to the PAS application.
- PAS Level 1 - allows the use of generic user ID and password to gain access.
- PAS Level 2 - requires a unique user ID and password to approve claims.

## APPENDIX A: FY 2002 COMMENTS AND RECOMMENDATIONS

---

During the course of our testwork, we noted the following areas for improvement related to the PAS information security controls:

1. At the time of our review in October 2002, 167 users had access to PAS. Of these 167 users, 138 (83 percent) no longer needed access. This situation was caused by OCGFC not removing user access when personnel terminated their employment with the OCGFC. As reported in our *Independent Auditor's Report on FEMA's FY 2002 Financial Statements*, FEMA's overall process for terminating users' system access needs improvement. Terminated employees who retain system access privileges can be a significant risk because they may be able to sabotage or otherwise impair agency operations or assets. Of the 138 users no longer requiring PAS access, 16 had the access privilege of Project Manager, which allowed them to approve claim payments.
2. Access to PAS Level 1 only requires a generic user ID and password. With this generic user ID and password, users can view and modify claim data, although they cannot approve claims. In addition, PAS Level 1 users can access claims under another reviewer's user account by selecting the reviewer's name from a drop down menu. Weak user system access controls such as these increase the risk of unauthorized access and reduces user accountability.
3. PAS password settings can be improved in several areas.
  - a. The system does not lock out users after a certain period of inactivity.
  - b. The system does not lock out users after three invalid attempts at PAS Level 2.
  - c. System passwords can be four characters in length at PAS Level 2 rather than the eight characters required by FEMA policy.
  - d. Users are not required to change their system passwords periodically.

Although sensitive PAS processing devices are in restricted areas, which helps reduce the risk of unauthorized access, good system password controls still should be maintained.

4. Standard change control documentation with appropriate management signatures does not exist for all PAS program changes. OCGFC officials said that program changes are approved via verbal communications and writing the change on a "whiteboard." We tested five system changes made during FY 2002, and we were informed that three of the changes were based on verbal authorizations and two were written on a "whiteboard" but subsequently erased. As a result, we could not verify that management approved the system changes.
5. PAS separation of duties should be strengthened. The PAS contractor continues to perform PAS programming functions, has access to the PAS test and production environments, has the ability to change data and assign security rights, and has personally submitted four Cerro Grande fire claims. Without appropriate separation of duties, OCGFC faces the risk of unintentional programming errors being entered into production, unauthorized or unpublished changes to PAS code, and entrance of viruses or malicious code into PAS.

## APPENDIX A: FY 2002 COMMENTS AND RECOMMENDATIONS

---

As a result of these issues, PAS is subject to additional risks of unauthorized disclosure, modification, or destruction of data.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, defines “information technology” as any equipment or interconnected system or subsystem used by the agency directly or used by a contractor under a contract with the agency. In addition, OMB Circular A-130 requires that Federal agencies implement technical controls in accordance with relevant National Institute of Standards and Technology (NIST) guidance. NIST’s September 1996 *Generally Accepted Principles and Practices for Securing Information Technology* guides that agencies should: 1) ensure that terminated employees’ system access is removed; 2) ensure that system users are required to uniquely identify themselves to the system before being allowed to perform any functions; 3) ensure systems limit the number of log-on attempts; and 4) implement separation of duties controls such that a single individual cannot subvert a critical process.

The GAO *Federal Information Systems Control Audit Manual (FISCAM)* requires that policies and procedures should be in place that prescribe who can authorize a system modification and how these authorizations are to be documented. The use of standardized change request forms helps ensure that requests are clearly communicated and that approvals are documented. The *FEMA Information Resources Management Policy and Procedural Directive (FIRMPD)* requires: 1) the suspension of a computer session (i.e., computer lockup) after ten minutes of inactivity; 2) a limit of three consecutive invalid log on attempts prior to lock out of computer users; 3) that agency system passwords be at least eight alphanumeric characters in length and should include at least one numeric character (0-9); and 4) that system passwords be changed at least once every 90 days.

We recommend that the OCGFC:

- 1.1 Review all OCGFC users who have access to PAS, lock any user accounts that are no longer needed, and ensure that a process is implemented to periodically review PAS users to ensure that only authorized individuals (e.g., current employees) have access to the system.
- 1.2 Ensure that the PAS Level 1 access controls are modified to create individual user login accounts and that the individual accounts have strong password controls.
- 1.3 Review PAS password parameters and modify them to:
  - a. Lock user computers after some reasonable period of time (e.g., ten minutes) of inactivity;
  - b. Lock out users after three invalid system log on attempts;
  - c. Ensure the use of eight alphanumeric password characters, with at least one numeric character, as required by the FIRMPD; and
  - d. Require that users change their system passwords every 90 days, at a minimum.
- 4.4 Establish a standard program change request form to document all PAS program changes, require prior documented management approval for all system changes, and perform a comprehensive review of PAS production programs to ensure that only management-approved programs are running in the production region.

- 4.5 Remove or, at least, closely monitor and control the access of the PAS contract application programmer from the production region of PAS and ensure a more detailed review of all claims submitted by personnel with access to PAS, including contractor personnel.

### 3. Mission Assignments and Interagency Agreements

Mission assignments are interagency agreements that are provided in anticipation of, or in response to, a Presidential Disaster Declaration. FEMA issues mission assignments to other Federal agencies stipulating performance of a specific task and including information such as funding, managerial controls, and guidance. Mission assignments are administered by the Disaster Finance Branch and other types of interagency agreements are administered by the Financial and Acquisition Management Division (FAMD).

During the course of our testwork, we noted the following improvements that could be made in the mission assignment and interagency agreement processes:

1. Of a sample of 15 mission assignments entered into during FY 2002, the Lead Accountant either did not perform or did not document the review of the Request for Federal Assistance (RFA), as required, for three RFAs.
2. Of a sample of 15 mission assignments closed during FY 2002, the FEMA project officer did not approve six RFAs issued to de-obligate the remaining funds.
3. A periodic reconciliation between ProTrac and the Integrated Financial Management Information System (IFMIS) was not performed to ensure the accurate transfer of programmatic and financial data between the systems. ProTrac is the system used by FAMD to track the interagency agreements open at any point in time.
4. No written policies and procedures exist for the monitoring and maintenance of interagency agreements.
5. Of a sample of 15 interagency agreements entered into during FY 2002, one of the files selected could not be located.

As a result of these issues, an increased risk exists that a mission assignment or interagency agreement will not be correctly processed and/or recorded.

The *Standards for Internal Control in the Federal Government* issued by the GAO requires that internal controls be implemented and that such controls be documented, and the Standard Operating Procedure (SOP) entitled *Processing Mission Assignments* requires that RFAs be reviewed and approved.

We recommend that FAMD:

- 1.1 Remind all appropriate personnel of the policies related to the review and approval of RFAs for both obligating and de-obligating actions and enforce such review requirements through a monitoring program.

- 1.2 Perform and document a periodic reconciliation between ProTrac and IFMIS. A supervisor should review this reconciliation.
- 1.3 Develop and implement agency-wide policies and procedures for the monitoring and close-out of interagency agreements. These policies and procedures should include a standardized filing system and documentation requirements to ensure the proper monitoring and maintenance of the interagency agreements.
- 1.4 Enhance document retention procedures to ensure that all interagency agreement files can be located timely.

#### 4. Grants Management

During the course of our testwork, we noted the following improvements that could be made to the grants management process:

##### *Region II*

1. At the end of each quarter, Region II personnel did not consistently reconcile in a timely manner total nondisaster grant obligations and disbursements between IFMIS and SmartLink.<sup>1</sup> Instead, these reconciliations were performed upon receipt of the Financial Status Reports (FSR). However, States or Commonwealths were occasionally delinquent in submitting their quarterly FSRs, leading to a delay in the preparation of the related reconciliations. Although reconciling the FSR, IFMIS, and SmartLink together may seem more efficient, the delay in reconciling IFMIS and SmartLink could lead to errors not being identified and corrected timely.
2. The second quarter reconciliations for two nondisaster grant programs were not performed correctly. In comparing total disbursements between IFMIS and SmartLink, not all disbursements made through the end of the quarter were considered.
3. A tracking mechanism for ensuring the receipt of all nondisaster grant FSRs was not used.

##### *Region IX*

4. Grant files were not properly maintained for Region IX's nondisaster grants. Several files that we requested could not be located, and overall the files lacked organization. For example, sections were not reserved for closeout documents, correspondence and reports were not in chronological order, and FSRs were missing.
5. Region IX personnel were unable to provide evidence of any monitoring of cash-on-hand balances maintained by grantees of nondisaster grants.
6. Region IX personnel did not perform any quarterly reconciliations between IFMIS, SmartLink, and the FSRs for the first, second, or third quarters of FY 2002 for the region's nondisaster grant programs.

---

<sup>1</sup>SmartLink is a subsystem of the Department of Health and Human Services' Payment Management System that FEMA uses to disburse grants.

## APPENDIX A: FY 2002 COMMENTS AND RECOMMENDATIONS

---

7. Region IX personnel did not track the receipt of FSRs related to nondisaster grants. As a result, certain requested FSRs could not be located.
8. Region IX personnel did not coordinate with the Northridge Long-Term Recovery Area Office to correct differences noted in FY 2002 reconciliations for the Northridge Disaster (Disaster #1008) public assistance grant program .
9. Disaster grant reconciliations between the amounts recorded as disbursements per the FSR and the amounts recorded in IFMIS and SmartLink were not completed properly.
10. Region IX was unable to provide documentation to support the extension or requests for extension for 8 of 13 Northridge hazard mitigation grant projects, likely as a result of poor record keeping.

The following require that accounts be reconciled timely and recorded accurately: the *Standards for Internal Control in the Federal Government* issued by the GAO; SOP entitled *Reconciling Grant Programs* issued by FAMD in March 1999; and Statement of Federal Financial Accounting Standards (SFFAS) No. 1, *Accounting for Selected Assets and Liabilities*, paragraphs 57 and 59. Untimely reconciliations could lead to delays in identifying and correcting errors related to obligations and disbursements.

We recommend that Region II and Region IX:

- 4.1 Implement a method for tracking nondisaster grant FSRs to help ensure that all activity related to nondisaster grants has been recorded properly.

We recommend that Region II:

- 4.2 Reconcile IFMIS and SmartLink promptly at the end of each quarter in accordance with the SOP, *Reconciling Grant Programs*, regardless of when the related FSRs are received, to ensure that nondisaster grants are properly recorded and de-obligated as funding is disbursed and received.
- 4.3 When performing the quarterly reconciliations for all nondisaster grant programs, ensure that the comparison of total disbursements between IFMIS and SmartLink consider all disbursements made through the end of the quarter.

We recommend that Region IX:

- 4.4 Develop and implement a method for organizing, filing, and monitoring its grant files to ensure that the files are complete, organized and available.
- 4.5 Develop and implement policies and procedures to monitor cash-on-hand balances of nondisaster grantees.
- 4.6 Reconcile all grant programs on a quarterly basis in accordance with the SOP to ensure that funds are de-obligated on a timely basis and that errors are resolved and corrected timely.

- 4.7 Record the appropriate adjustments based on the FY 2002 reconciliations of Disaster #1008's Public Assistance grant to ensure that this grant's activities and balances are properly reflected in IFMIS.

In addition, Region IX personnel should coordinate with the Northridge Long-Term Recovery Area Office in reconciling cumulative grant expenses and obligations for Disaster #1008 and correcting any identified variances on a quarterly basis.

- 4.8 Develop and implement procedures to ensure that disaster grant reconciliations between the amounts recorded as disbursements per the FSR and the amounts recorded in IFMIS and SmartLink are completed properly.
- 4.9 Develop and implement policies and procedures to ensure that appropriate documentation is on hand to support extensions of hazard mitigation grants.

## 5. Budget Reprogrammings

During the course of our testwork, we noted the following improvements that could be made related to budget reprogrammings:

1. FEMA should review and, if necessary, update its policies and procedures for identifying, communicating, and recording reprogrammings to ensure the consistency and accuracy of their application.
2. FEMA's Congressional & Intergovernmental Affairs Division did not consistently follow its internal policies and procedures relating to the retention of correspondence with Congress for reprogrammings.

The *Standards for Internal Control in the Federal Government* issued by the GAO states that internal controls include the policies, procedures, techniques, and mechanisms that enforce management's directives.

We recommend that:

- 5.1 FAMD develop and implement written policies and procedures for the reprogramming process that include, but are not limited to, the following information:
- a. The definition and proper identification of reprogrammings;
  - b. The individuals in FAMD who are responsible for performing reprogrammings; and
  - c. The procedures to communicate with Congress and OMB to obtain approval prior to executing reprogrammings when necessary.
- 5.2 The Congressional & Intergovernmental Affairs Division enforce its procedures to document and retain all written and oral communication with Congress regarding reprogrammings.

## 6. Information Technology –Region II

During the course of our testwork, we noted the following areas where information technology (IT) controls could be improved:

1. We tested ten User Access Request (UAR) forms for the National Emergency Management Information System (NEMIS) and noted that one user approved her own UAR. Although this case appeared to be an exception, such a control weakness could lead to unauthorized access to critical data. Region II officials noted that the employee only granted herself print access, not system-processing access. However, under no circumstances should end users approve their own system access rights.
2. The Region II Continuity of Operations Plan (COOP) had not been updated since September 2000. We noted that several of the points of contact in the COOP were not current, and critical regional personnel did not maintain copies of the COOP off-site. Consequently, critical personnel may not know who to contact or know all their responsibilities in the event of a disaster. Although Region II had a system and data backup process, a current and complete COOP is needed should a significant system or data center outage occur.

OMB Circular A-130 requires that Federal agencies implement technical security controls in accordance with NIST guidance. NIST, in its September 1996 *Generally Accepted Principles and Practices for Securing Information Technology Systems*, guides that organizations should: 1) implement adequate separation of duties such that a single individual cannot subvert a critical process; and 2) keep contingency plans current and periodically test and revise contingency plans. A business continuity plan such as the COOP is a key component of an organization's overall contingency planning strategy.

We recommend that Region II:

- 1.1 Remind all personnel that all system UARs must be approved by a manager who is not the access requester.
- 1.2 Continue with plans to work with the Office of National Preparedness to update the Region II COOP.

## 7. IFMIS

Three FEMA contract employees and one FEMA employee share the same highly privileged IFMIS user account that is used to migrate IFMIS software code into production. We inquired with the Information Technology Services Directorate, Office of Cyber Security, and noted that during FY 2002, a waiver for this group account had not been approved by the FEMA Chief Information Security Officer (CISO), as required by the FIRMPD. However, subsequent to the completion of our audit, a waiver was approved by the CISO. Therefore, we have no recommendation at this time.



**APPENDIX B: SUMMARY STATUS OF COMMENTS REPORTED IN THE FY 2001 MANAGEMENT LETTER**

FY 2001 Management Letter Recommendation Number.	Location/ Office	Audit Area	Description of Audit Finding	Implementation Status of Recommendations as of September 30, 2002	Rationale, If Recommendation Considered Open
1.1	OCGFC	Cerro Grande Administration	Lack of sufficient documentation for claims	Implemented and closed	N/A
1.2	OCGFC	Cerro Grande Administration	Duplication of benefit searches	Implemented and closed	N/A
1.3	OCGFC	Cerro Grande Administration	Lack of detailed assessments of the EDP controls supporting ACIS or the contractor's data center in New Jersey	Expanded and included in the FY 2002 internal control report	N/A
1.4	OCGFC	Cerro Grande Administration	ACIS user password history feature is not activated	Not implemented and open	Condition cited continues to exist.
1.5	OCGFC	Cerro Grande Administration	Claims audited by the comptroller did not always represent 20 percent of claims to be paid	Implemented and closed	N/A
1.6	OCGFC	Cerro Grande Administration	Significant time lag between determination and communication of overpayments by OCGFC to the Disaster Finance Branch (DFB) and to the claimant	Implemented and closed	N/A
1.7	OCGFC	Cerro Grande Administration	Two of 28 commitment forms (FEMA Form 40-1) tested were not approved by both the program head and the comptroller	Implemented and closed	N/A
2.1	HRD	Human Resources	Based on a sample, leave audits were either not conducted at the end of pay period 13 or the leave audit performed was not documented	Not implemented and open	Condition cited continues to exist.

**APPENDIX B: SUMMARY STATUS OF COMMENTS REPORTED IN THE FY 2001 MANAGEMENT LETTER**

2.2	Headquarters/ HRD, Headquarters/ ITSD and Headquarters/ FAMD	Human Resources	Electronic Data Processing controls for QuickTime system can be improved	Implemented and closed	N/A
3.1	Regions V and VI	Grants Management	Reconciling grant programs	Not implemented and open	Insufficient time to implement recommendation during FY 2002.
3.2	Region V and Headquarters/ FAMD	Grants Management	Recording of Project Impact expenses	Implemented and closed	N/A
3.3	Headquarters/ ITSD and Headquarters/ HRD	Grants Management	Nine employees identified by information obtained from FEMA as being terminated still had active access to NEMIS	Expanded and included in the FY 2002 internal control report	N/A
4.1	Headquarters/ FAMD	Reimbursable Agreements	Inadequate process for determining accounts receivable related to individual reimbursable agreements	Not implemented and open	Condition cited continues to exist.
4.2	Headquarters and DFB/ FAMD	Reimbursable Agreements	Advance balances exist for certain agreements with expired performance periods	Implemented and closed	N/A
4.3	DFB/FAMD	Reimbursable Agreements	Improve control procedures over Fund 27 reimbursable agreements	Partially implemented and closed; see related FY 2002 recommendation #4.1	N/A

**APPENDIX B: SUMMARY STATUS OF COMMENTS REPORTED IN THE FY 2001 MANAGEMENT LETTER**

5.1	DFB/FAMD	Grants Management - Accounts Receivable	Lack of written policies and procedures for the periodic determination of the allowance for uncollectible accounts	Partially implemented and open	Although written procedures now exist, we did not find evidence that these procedures were fully implemented at September 30, 2002. In addition, the written procedures do not include individual account analysis.
6.1	Headquarters and DFB/FAMD	Various - Accounts Payable Accrual	Double-counting of certain invoices in the accounts payable accrual; certain expenses omitted from the accrual	Expanded and included in the FY 2002 internal control report	N/A
7.1	Headquarters and DFB/FAMD	Property Management	Building improvements are depreciated over 20 years without consideration of the remaining useful life of the related buildings	Partially implemented and open	Based on FAMD's review of all Property Plant & Equipment as part of its nationwide equipment inventory, the balance for this asset class was corrected to remove erroneous items. However, no specific changes were made to FAMD's depreciation methodology for this asset class.

**APPENDIX B: SUMMARY STATUS OF COMMENTS REPORTED IN THE FY 2001 MANAGEMENT LETTER**

8.1	Headquarters/ FAMD; Emmitsburg/ United States Fire Admin- istration; Headquarters/ ITSD; Headquarters/ National Secu- rity Division	Performance Measures	Lack of written policies and procedures	Implemented and closed	N/A
8.2	Headquarters/ FAMD	Performance Measures	FEMA's performance reporting for FY 2001 could be improved	Implemented and closed	N/A
9.1	Headquarters/ FAMD	Financial Reporting	Required risk assumed information relating to the National Flood Insurance Program	Implemented and closed	N/A
10.1 and 10.2	Headquarters/ FAMD, Headquarters/ ITSD	IT Controls	Joint Financial Management Improvement Program certified version of IFMIS could not be verified	Implemented and closed	N/A
11.1	Headquarters/ FAMD	Laws and Regulations	Primary sources of information for the annual assurance statements of selected FEMA managers were audits conducted by external parties and the Office of the Inspector General	Not implemented and open; noncompliance with the Federal Manager's Financial Integrity Act cited in FY 2002 compliance report	Condition cited continues to exist.

We received written comments on the draft of our management letter from the following FEMA management officials:

- Director, Office of Cerro Grande Fire Claims (OCGFC)
- Assistant Director/Chief Information Officer, Information Technology and Services Directorate (ITSD)
- Acting Regional Director, Region II
- Regional Director, Region IX
- Acting Chief Financial Officer, Financial and Acquisition Management Division (FAMD)

These written comments are presented in Appendices D through H. FEMA officials generally expressed agreement with the findings and recommendations of the draft management letter and indicated that in some cases, corrective actions had been taken or were underway. In other instances, management presented other information and we made changes to the report as appropriate or have provided our analysis of those comments as follows:

### OCGFC

Regarding our recommendation 2.1 to lock any Payment Approval System (PAS) user accounts that are no longer needed, OCGFC instead plans to delete these accounts. For future issuances of user accounts, OCGFC plans to issue them only on a short-term, interim basis, and to review and validate all user accounts on a quarterly basis to ensure that unneeded users accounts are removed. OCGFC also plans to remove user accounts for any employees immediately following their departure.

Regarding our recommendations 2.3(a) through 2.3(d) to modify PAS password parameters, OCGFC states that they do not plan to implement recommendation 2.3(a), but do plan on implementing recommendations 2.3(b), 2.3(c), and 2.3(d). Recommendation 2.3(a) calls for locking user computers after ten minutes of inactivity. However, OCGFC states that implementing this recommendation would require “some expense and system downtime” and would, therefore, not be practical to perform. We believe that our recommendation 2.3(a) could be implemented even without extensive modifications to the PAS software. For example, the individual personal computer station can be easily modified to include password protected screen savers that would restrict access by any unauthorized user, yet allow the user to perform all the necessary offline activities stated in OCGFC’s response. We plan to, therefore, continue recommending that OCGFC revisit their response and determine some practical implementation of our recommendation 2.3(a).

Regarding our recommendation 2.5 to remove, or closely monitor and control, the access of the PAS contract application programmer from the production region of PAS, OCGFC states that they will continue to monitor all contractor activity and ensure the required review and approval of all PAS payment activity. OCGFC states, furthermore, that based on their oversight of the contractor’s activities, they do not plan to terminate this contractor. Our recommendation did not call for this contractor to be terminated, but did call for close monitoring and control of his activities. As long as OCGFC continues to implement this part of our recommendation, we do not disagree with OCGFC’s decision to retain this contractor.

## APPENDIX C: ANALYSIS OF MANAGEMENT COMMENTS

---

### FAMD

Regarding our recommendation 5.1 to review and update their policies and procedures guidance related to budget reprogrammings, our initial recommendation was that FAMD should prepare such guidance. However, FAMD provided their most current guidance related to such activity and we, therefore, modified our initial recommendation to instead suggest that FAMD review and, if necessary, update their current guidance.




## Federal Emergency Management Agency

Washington, D.C. 20472

June 27, 2003

### MEMORANDUM

TO: J. Richard Berman  
Assistant Inspector General for Audits

FROM: Matt Jadacki   
Acting Chief Financial Officer  
Emergency Preparedness and Response Directorate

SUBJECT: Draft Management Letter for FEMA's Fiscal Year 2002  
Financial Statement Audit  
Audit Report A-03-03

Thank you for the opportunity to provide comments on the Draft Management Letter. While in agreement with most comments and recommendations, there was an area that the OIG and their contractor need to reconsider.

The item is Appendix A – 6. Budget Reprogrammings. The finding was that FEMA did not have written policies and procedures for identifying, communicating, and recording reprogrammings. Section 8-3 of the FAMD budget handbook addresses reprogrammings. If KPMG is referring to system guidelines for entering and identifying reprogrammings, this is not an item that needs to be addressed. There are many changes under the reprogramming guidelines each year that may not trigger a reprogramming request until the last entry. For example, if the limit for a reprogramming is \$500,000, and during the course of the year \$150K, \$250K, and \$100K are moved to another activity, it is not until the last \$100K that a reprogramming is required.

If you have any questions or need further information concerning our response, please contact me at (202) 646-3545 or Kaye McTighe at (202) 646-4231.



Federal Emergency Management Agency

Washington, D.C. 20472

JUL 14 2003

MEMORANDUM FOR: J. Richard Berman  
Assistant Inspector General for Audits

FROM: Rosita O. Parkes *Rosita O. Parkes*  
Assistant Director  
Information Technology Services Directorate

SUBJECT: Draft Management Letter for FEMA's Fiscal Year  
2002 Financial Statement Audit Report A-03-03

The Information Technology Services Directorate (ITSD) appreciates the opportunity to review the Draft Management Letter for FEMA's Fiscal Year 2002 Financial Statement Audit Report A-03-03. We agree with the recommendations.





## Office of Cerro Grande Fire Claims

Post Office Box 90215  
Denton, Texas 76202  
Claims Information Helpline: 1-888-748-1853

July 3, 2003

Mr. J. Richard Berman  
Assistant Inspector General for Audits  
Office of Inspector General  
Department of Homeland Security  
Washington, D.C. 20528

Re: Draft Management Letter for FEMA's Fiscal Year 2002  
Financial Statement Audit, Audit Report A-03-03

Dear Mr. Berman:

Thank you for your June 5, 2003, memorandum, which forwarded your draft Audit Report entitled "Management Letter for FEMA's Fiscal Year 2002 Financial Statement Audit", Audit Report A-03-03. I am writing in response to the recommendations in the draft report which relate to the administration of the fire claims processing activities of the Office of Cerro Grande Fire Claims (OCGFC). We are pleased to report we have already undertaken action on several of the recommendations included under Appendix A, Paragraph 2, of that report, and we are nearing completion of corrective actions on those recommendations. In the balance of this letter I will provide a brief description of our activity on each of the OIG recommendations.

In Paragraph 2.1 of Appendix A of the draft report you recommend that OCGFC "Review all OCGFC users who have access to PAS, lock any user accounts that are no longer needed, and ensure that a process is implemented to periodically review PAS users to ensure that only authorized individuals (e.g., current employees) have access to the system." In response to this recommendation we have reviewed the user accounts appearing in the system and, rather than locking those accounts no longer needed, plan to remove such user accounts. Any authorized personnel who may require system access in future can be added on an interim, short-term basis, and those accounts can be removed when access is no longer required. After the initial account adjustments, which we have targeted for this month, the Director of OCGFC will assign responsibility to a full-time OCGFC staff member to review and validate system access on a quarterly basis. We will also impose the requirement to adjust the access as required immediately following the departure of any authorized users who may have had access privileges. Any user account deletions or additions and/or reviews and adjustments to access will be

## APPENDIX F: MANAGEMENT COMMENTS - OGFC

---

coordinated with the IT Systems Director at the Texas National Processing Service Center (NPSC), who maintains the PAS server and provides local technical support.

Appendix A, Paragraph 2.2, of the draft report contains a recommendation that OCGFC "Ensure that the PAS level 1 access controls are modified to create individual user login accounts and that the individual accounts have strong password controls." In response to this recommendation we have coordinated software changes to modify PAS level 1 access controls with individual user login accounts and passwords in compliance with FEMA Resources Management Policy and Procedural Directive (FIRMPD), and we have conducted an initial field test on our PAS. Following finalization of software refinements and installation of the modifications, we will coordinate monitoring procedures to ensure the maintenance of continued strong password controls with the IT Systems Director at the Texas NPSC, who maintains the PAS server and provides local technical support.

Appendix A, Paragraph 2.3, of the draft report contains several recommendations relating to PAS password parameters. The recommendations are to: a) "Lock user computers after ten minutes of inactivity;" b) "Lock out users after three invalid system log on attempts;" c) "Ensure the use of eight alphanumeric password characters, with at least one numeric character", and d) "Require that users change their system passwords every 90 days, at a minimum."

We have some concerns about the recommendation that computers be locked after ten minutes of inactivity. We believe that this would require some expense and system downtime requiring individual software form implementation. PAS was not designed to be a "continuous activity" system. This is due to the requirement for reading and research of sometimes extensive and complex paper-based Payment Recommendation packages, offline confirmation of calculations, and other production, review and approval activities not directly associated with authorized entry or modification of data contained in the system. We therefore do not intend to implement this recommendation. However, we would be pleased to discuss this recommendation with you to see if there is some way to address your concern and, at the same time, continue to process claims payments efficiently.

We accept your recommendation relating to locking out users after three invalid log on attempts, so we have designed software modifications with password parameters to lock out users after three invalid system log on attempts. We are coordinating the installation of these modifications with the IT Systems Director at the Texas NPSC, who maintains the PAS, and we expect this modification will be completed this month.

With respect to your recommendation that we ensure the use of eight password characters, with at least one numeric character, we have taken steps to implement software modifications with password parameters to force the use of eight alphanumeric password characters with at least one numeric character. We will coordinate the installation of these modifications with the IT Systems Director at the Texas NPSC, who maintains the PAS.

With respect to your recommendation about password changes, we are nearing completion on software modifications to require user password changes at a minimum of each 90 days. We are coordinating the installation of these modifications with the IT Systems Director at the Texas NPSC, who maintains the PAS. We expect to complete this process this month.

Appendix A, Paragraph 2.4, of the draft report recommends that OCGFC “Establish a standard program change request form to document all PAS program changes, require prior documented management approval for all system changes, and perform a comprehensive review of PAS production programs to ensure that only management-approved programs are running in the production region.” We anticipate few PAS program changes this late in the Cerro Grande fire claims program. Due to the relatively small size of the program, past PAS program changes have been coordinated without a standard program change request form. However, we agree that such a form would serve to establish a more formal record of management approval for system changes. We have conducted initial discussions with the IT Systems Director at the Texas NPSC to obtain a standard program change request form, and we will use such a form for future PAS program changes.

Appendix A, Paragraph 2.5, of the draft report recommends that OCGFC “Remove access of the PAS contract application programmer from the production region of PAS and ensure a more detailed review of all claims submitted by personnel with access to PAS, including contractor personnel.” While it is true that our application program contractor has access to the PAS and previously submitted claims that are now closed, we do not believe that these circumstances dictate a need to terminate the contractor. OCGFC initiates and closely monitors all contractor activity, including system modifications. The contractor is not co-located in the production office; he provides services on an as-needed basis from New Mexico, supplemented by occasional trips to our office, and those visits are initiated and closely monitored by OCGFC staff. After successful completion of OIG recommendations and modifications to the PAS, which requires liaison with the programmer, OCGFC will grant the programmer access to the production region of PAS only in limited circumstances, and only with oversight by OCGFC staff. We believe that OCGFC has, by layered authority safeguards, assured program compliance on all claims submitted by personnel with access to PAS. Production, Processing and Approval Officials were aware of a small number of OCGFC personnel with PAS access who were also claimants because they were hired locally after the Cerro Grande Fire. These Officials evaluated the merit of those claims with the same level of scrutiny used in all claims. Once an Authorizing Official approves the payment of a claim, PAS ensures that payment cannot be altered or modified by anyone without the “rights” of an Authorizing Official. For these reasons we believe it is not necessary to terminate this OCGFC contractor.

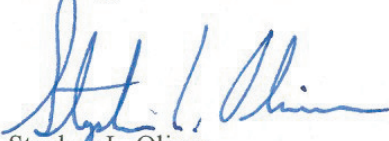
In summary, with the exception of the recommendations relating to locking out users after ten minutes of inactivity and replacement of an OCGFC contractor, we plan to complete implementation of the system modifications that your draft audit report recommends in the near future.

**APPENDIX F: MANAGEMENT COMMENTS - OGFC**

---

Thank you for your recommendations and for the assistance provided to the Office of Cerro Grande Fire Claims by the OIG staff. Please call me at (940) 891-8799 after you have had an opportunity to review this response to the draft audit report if you have any further questions.

Sincerely,



Stephen L. Oliver  
Director

Office of Cerro Grande Fire Claims

cc: Matt Jadacki  
Acting Chief Financial Officer  
Emergency Preparedness and Response Directorate

Rose Parkes  
Chief Information Officer  
Emergency Preparedness and Response Directorate



Federal Emergency Management Agency

Region II  
26 Federal Plaza  
Room 1311  
New York, NY 10278-0002

July 2, 2003

**MEMORANDUM FOR:** Nancy L. Hendricks  
Deputy Assistant Inspector General for Audits  
Office of Inspector General

A handwritten signature in cursive script, appearing to read "Joseph F. Picciano".

**FROM:** Joseph F. Picciano  
Acting Regional Director  
FEMA Region II

**SUBJECT:** Draft Management Letter for FEMA's Fiscal Year 2002  
Financial Statement Audit  
Audit Report A-03-03

Attached are our comments on the subject draft audit report.

The Administration & Resource Planning Division and the National Preparedness divisions in Region II have reviewed this report.

Reference pages:

A-5 issues with grants management  
A-6 recommendations for Region 2  
A-7 COOP issues and IT issues  
A-7 recommendation for Region 2

A-5/A-6 issues with grants management

Finding/Recommendation #1:

Corrections have already been made for FY 2003 grant awards. Reconciliation of the remaining FY 2002 grant award files will be completed by July 15, 2003. The FY 2001 and 2000 grant awards that had not been reconciled are presently being completed. We expect to have the reconciliation of all prior year grant awards completed by September 30, 2003.

A spreadsheet for tracking the Financial Status Reports (FSRs) was in place during the auditing period, however it was not being fully utilized. Since the audit, this spreadsheet has been updated to add the additional grants awarded to date, and is now current for the FY'2003 grant files. This tracking mechanism is also being utilized for the remaining prior year grant files to monitor FSR submissions.

As a result of the utilization of this tracking mechanism, we have been able to immediately notify each State when they are delinquent with an FSR submission. We also have the capability to identify those prior year FSRs that are missing. This process, consistent with the recommendation, will now be standard practice for the Region.

Finding/Recommendation #2:

Quarterly IFMIS and Smartlink reconciliations are current for grant awards issued during FY 2003. There are six files pending reconciliation from FY 2002, and these will be completed by July 15, 2003. Reconciliations for FY 2001 and 2000 grant awards, that had not been reconciled, are presently being completed. We expect to have the reconciliation of all prior year grant awards completed by September 30, 2003.

The Region has initiated implementing the procedure of reconciling IFMIS and Smartlink on a quarterly basis, even in the event the State Financial Status Report (FSR) has not been received. Upon receipt of each State's FSR, the quarterly IFMIS/Smartlink reconciliations previously performed are then matched/reconciled with the respective FSR. As a result of these reconciliations, we will be expanding the program notification process beyond the EMPG award, which will notify other program officers when funding has not been expended by the State. This process will also serve to expedite the identification and deobligation of grant funds that are no longer required by the grant recipient.

Finding/Recommendation #3:

Corrections have been made. The tracking mechanism is now in place. In regard to the specifics with this finding, final FSRs for the two program years in question have been submitted, and corrected. All disbursements have been considered for the

aforementioned two program years, and the grant closeouts are in process. Quarterly disbursements for all other grant programs were and continue to be considered during our IFMIS/Smartlink reconciliation process.

It should be noted that by FEMA headquarters combining the NJ TCMFA funds for FY 2000 and 2001 into the same Smartlink account contributed to the finding in this area, although the Region recognizes the need for improved tracking.

**A-7 COOP issues and Information Technology issues**

Finding/Recommendation #1: We have further controlled the User Access Request form for the National Emergency Management Information System (NEMIS). The primary responsibilities for requesting access have been transitioned to the various program area managers/supervisors. Information Technology (IT) will only serve as the last resort for approvals if and when the User Access Request form is signed or e-mailed by an authorized requesting official. All IT personnel have been reminded that an authorized manager must approve requests. The approval, which was represented in the audit report, did not grant or authorize the individual access to any NEMIS or IFMIS data. Access was granted in this case for local server access only allowing them to print to a network printer.

Finding/Recommendation #2: The (COOP) plan is the responsibility of the Region's National Preparedness Division. The Region II Continuity of Operations Plan (COOP) has been updated and provided in draft form to all employees. The final version will be ready for distribution by the end of June of 2003. On site training at the Region's pre-identified COOP site is presently ongoing on a rotational basis for all regional division staff.



## Federal Emergency Management Agency

Region IX  
1111 Broadway Suite 1200  
Oakland, California 94607-4052

**JUL 14 2003**

MEMORANDUM FOR: J. Richard Berman  
Assistant Inspector General for Audits

From: Jeff Griffin *Kevin J. Clark for*  
Regional Director

Subject: Draft Management Letter for FEMA's Fiscal Year 2002  
Financial Statement Audit  
Audit Report Number A-03-03

In response to your June 5, 2003 memorandum to Region IX regarding specific findings related to the Financial Statement Audit, the following is provided as additional action and information to your recommendations.

### Appendix A – FY2002 Comments and Recommendations:

- 5.1 Implement a method for tracking nondisaster grant FSRs to help ensure that all Activity related to nondisaster grants has been recorded properly.

*FEMA Response:* Region IX is currently using a nondisaster spreadsheet that contains a section for tracking FSRs. Staffing resources have been redirected to assist in this area.

- 5.4 Develop and implement a method for organizing, filing, and monitoring its grant files to ensure that the files are complete, organized and available.

*FEMA Response:* Address any deficiencies in the older files and process reconciliation & final closure of the grants. All reports pertaining to the reconciliation and closure will be filed in the individual files. Management is redirecting staff resources to assist with this effort and will have files maintained and properly organized during this fiscal year.

- 5.5 Develop and implement policies and procedures to monitor cash-on-hand balances of nondisaster grantees.

*FEMA Response:* The region has developed a spreadsheet and is entering the data that will serve as a monitoring tool. The spreadsheet will provide the cash-on-hand analysis. All reports (IFMIS, SMARTLINK, FSR20-10) used for the data entry to the spreadsheet



will be filed in the individual grant files. Also, for grantees that do not use SMARTLINK for reimbursement, but file a Request for Reimbursement (SF270), a liquidation sheet will be used to track expenditures along with the necessary IFMIS reports (header sheet, cross reference report). Management is redirecting staff resources to assist with the data entry and filing.

- 5.6 Reconcile all grant programs on a quarterly basis in accordance with the SOP to ensure that funds are de-obligated on a timely basis and that errors are resolved and corrected timely.

*FEMA Response:* Region IX has developed the quarterly reconciliation worksheet and established reconciliation procedures to ensure that adjustments and corrections are processed on a timely manner, and errors are rectified and resolved on a timely basis.

- 5.7 Record the appropriate adjustments based on the FY2002 reconciliation of Disaster 1008 Public Assistance Grant to ensure that this grant's activities and balances are properly reflected in IFMIS.

*FEMA Response:* Region IX has developed the spreadsheet to track and monitor Disaster 1008 Public Assistance Grant activities, and is used to track grant obligations posted in IFMIS that has been released to SMARTLINK. Reconciliation of cumulative obligations and expenses has been performed and completed as of FY2003 quarter ending June 30, 2003. The Regional Grant Management staff and NLTRA Office are working together in a collaborative effort to identify variances and rectify such in a timely manner. The regional staff is providing the NLTRA Office with copies of financial reconciliation. This corrective action will continue until DR1008 is closed and transitioned to the regional office.

- 5.8 Develop and implement policies and procedures to ensure that disaster grant reconciliation between the amounts recorded as disbursements per the FSR and the amounts recorded in IFMIS and SMARTLINK are completed properly.

*FEMA Response:* Reconciliation worksheet has been developed and revised to include a section for FSR (FF20-10) data. The worksheet provides all the financial activities of the disaster grants and reconciliation of the disaster disbursement and obligation as recorded in IFMIS, SMARTLINK, PROGRAM DATABASE (Adams/Nemis) and FSR (FF20-10 / PMS 272).

- 5.9 Develop and implement policies and procedures to ensure that appropriate documentation is on hand to support extensions of hazard mitigation grants.

*FEMA Response:* Region IX is implementing headquarters established policies and procedures for extensions on hazard mitigation grant projects. An unliquidated obligation-tracking log has been developed to track all hazard mitigation projects.

If you have any questions on this memorandum, please contact Kevin Clark at (510) 627-7102.

## APPENDIX I; OIG CONTRIBUTORS TO THIS REPORT

---

Sue Schwendiman, Director  
Vonna Holbrook, Audit Manager  
Charles Egu, Auditor



## APPENDIX J: REPORT DISTRIBUTION

---

Michael D. Brown  
Under Secretary  
Emergency Preparedness and Response

Patrick Rhode  
Chief of Staff  
Emergency Preparedness and Response

Matt Jadacki  
Acting Chief Financial Officer  
Financial and Acquisition Management Division

Barry C. West  
Chief Information Officer  
Information Technology and Services Directorate

Lea Ann McBride  
Acting Director  
Office of Public Affairs

Daniel A. Craig  
Director  
Recovery Division

Douglas G. Fehrer  
Director  
Human Resources Division

Joseph Picciano  
Acting Regional Director  
Region II

Jeff Griffin  
Regional Director  
Region IX





### **Additional Information and Copies**

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at [www.dhs.gov](http://www.dhs.gov).

### **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 the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.