OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Needs to Improve Change Controls for Integrated Financial Management System

Report No. 2004-P-00026

August 24, 2004

Report Contributors:

James Rothwell
Anita Mooney
Neven Morcos

Abbreviations

CMS	Change Management System
CFO	Chief Financial Officer
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FDW	Financial Data Warehouse
GAO	Government Accountability Office
IFMS	Integrated Financial Management System
NIST	National Institute of Standards and Technology
OARM	Office of Administration and Resources Management
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
RACF	Resource Access Control Facility

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

August 24, 2004

MEMORANDUM

SUBJECT: EPA Needs to Improve Change Controls for Integrated Financial Management System
Assignment No. 2003-000909
Audit Report No. 2004-P-00026

FROM: Patricia H. Hill, Director /s/
Business Systems Audits (2421T)

TO: Charles E. Johnson, Chief Financial Officer
Office of the Chief Financial Officer (2710)

David O'Connor, Acting Assistant Administrator
Office of Administration and Resources Management (3101A)

This is our final report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and the findings contained in this report do not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days of the date of this report. You should include a corrective actions plan for agreed upon actions, including milestone dates. We have no objections to the further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0894, or James Rothwell, Assignment Manager, at (202) 566-2570.

cc: Lorna McAlister, OCFO
Kristina Mainess OCFO
Juanita Galbreath, OCFO
Rich Lemley, OARM
Sandy Womack, OARM
Wes Carpenter, OARM

Executive Summary

Purpose

We conducted this audit to evaluate the adequacy of Environmental Protection Agency (EPA) Office of the Chief Financial Officer (OCFO) policies, procedures, and practices for controlling financial application development and software changes to EPA's Integrated Financial Management System (IFMS). IFMS is integral to the preparation of the Agency's financial statements. We evaluated operational management and security controls used to govern software modifications for this system to address the following questions:

- Do security controls provide reasonable assurance that access to software libraries is limited to authorized individuals and, consequently, that software modifications are properly controlled?
- Do the operational controls provide reasonable assurance that system software modifications and processing features are properly authorized?
- Do the operational controls ensure all new and revised software is properly tested and approved before it is placed into production?

Results of Review

We found a general breakdown of security controls that could undermine the integrity of IFMS software libraries and financial system data. Duties were not adequately segregated, individuals used an inappropriate ID or continued to have system access after no longer needing it, and contractor personnel were granted access to IFMS without a successful background security check. Numerous accountability and contractual issues contributed to this, including OCFO not having a system for identifying employee responsibilities related to IFMS security, and management not performing a risk assessment of IFMS's general support system. As a result, there was a high risk that system programmers could make unauthorized or unapproved changes to system software and data used for EPA's accounting and financial reporting.

Also, OCFO is not managing the contract for IFMS software modifications in a manner that ensures the proper authorization, acceptance, and approval of all new and revised software. OCFO management is not properly using its Change Management System to manage change activities for IFMS and provide technical direction to contractor staff. Although we had previously identified contract management problems, OCFO continued to use contract practices that gave the appearance of an improper personal service relationship with the contractor. A personal services relationship was clearly demonstrated when OCFO Financial

Systems Staff orally instructed the contractor to bypass documented channels and correct erroneous transactions totaling over $222 million by entering negative debits and positive credits “directly” into IFMS.

Further, OCFO management has not instituted a formal, structured change control process for IFMS to ensure software program modifications are properly authorized, tested, and approved. Such controls are needed to reduce the risk of unauthorized programs or modifications being implemented, and to provide for system security certification and accreditation. However, OCFO management did not implement formal change controls, as agreed to in a 1998 Office of Inspector General report. Inadequate change controls over IFMS software modifications places the Agency at risk that the availability, confidentiality, and integrity of EPA’s accounting and financial reporting functions could be compromised.

Recommendations

We are making various recommendations to OCFO to improve IFMS controls. In particular, we recommend that OCFO perform a risk assessment of the Endevor system used to control IFMS development, testing, and maintenance, and develop a security plan for Endevor. We also recommend that OCFO remove access for all contractor personnel without a pending personnel security screening request or a final acceptable background check. Further, we recommend that OCFO establish a systematic process for identifying key responsibilities, and holding employees accountable. In addition, we recommend that the Acting Assistant Administrator for Administration and Resources Management finalize pertinent guidance and procedures.

Agency Response and OIG Comments

The Chief Financial Officer concurred with our recommendations and generally outlined appropriate corrective actions to improve security and change controls over IFMS. The Acting Assistant Administrator for Administration and Resources Management did not concur with our recommendations concerning contractor background investigations, asserting that “suitability” background investigations of Federal contractors are not required. Management stated its existing, interim procedures were sufficient to guide offices that chose to initiate background investigations. However, current EPA policy and Federal guidance strongly recommend screening comparable to that for Federal staff, and we strongly urge such screening. The Federal government is operating in a high risk environment, and extra care needs to be taken to ensure non-Federal workers have acceptable backgrounds before trusting them with access to sensitive data and systems.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

We conducted this audit to evaluate the adequacy of Environmental Protection Agency (EPA) Office of the Chief Financial Officer (OCFO) policies, procedures, and practices for controlling financial application development and software changes to EPA's Integrated Financial Management System (IFMS). We evaluated operational management and security controls used to govern software modifications for this system to address the following questions:

- Do security controls provide reasonable assurance that access to software libraries is limited to authorized individuals and, consequently, that software modifications are properly controlled?

- Do the operational controls provide reasonable assurance that system software modifications and processing features are properly authorized?

- Do the operational controls ensure all new and revised software is properly tested and approved before it is placed into production?

Background

IFMS is a customized version of Federal Financial System software, which is maintained and modified through contracted services. The contract requires EPA to use its Change Management System to identify and prioritize changes to IFMS system software. EPA purchases vendor updates for IFMS through an annual licensing agreement. EPA controls the changes to IFMS by grouping them into a sub-release; to date, EPA has implemented 10 sub-releases to IFMS.

The integrity of IFMS data is integral to EPA's financial management operations because it is the central system and interfaces with numerous other administrative, financial, and mixed financial systems. IFMS supports such core financial management activities as general ledger, budget execution, funds control, accounts payable, disbursements, accounts receivable and collections, travel and project cost accounting, fixed assets, and standard reporting functions.

Scope and Methodology

We conducted this audit from May 2003 to March 2004 in accordance with *Government Auditing Standards,* issued by the Comptroller General of the United States. Our work was performed with Agency officials at EPA Headquarters in Washington, DC. In addition, we performed work with the Financial Data Warehouse system manager and the Delivery Order Project Officer for the facility support contract at Research Triangle Park, North Carolina. We also obtained and reviewed contract documents from the General Services Administration that pertained to the Inter-Agency Grant for maintaining and operating the Endevor system.

To evaluate the IFMS software libraries' security controls, we reviewed IFMS's security plan, and evaluated personnel screening procedures for systems contractor staff. We also tested and observed Endevor operational security procedures for monitoring and moving software changes made in 2003. Further, we tested and observed Resource Access Control Facility (RACF) security used in 2003 for access to IFMS libraries.

To determine whether IFMS operational controls provided reasonable assurance that software modifications were properly authorized, we reviewed: Federal regulations, Agency and OCFO policies, the IFMS Security Plan, and pertinent contract documents. Specifically, we evaluated contract administration for seven software development tasks during fiscal 2003, as well as the approval process used by EPA prior to placing these changes into production. We reviewed similar documents to determine whether IFMS operational controls ensure that new and revised software are properly tested and approved prior to being implemented. Specifically, we evaluated the testing and approvals for the seven system software modifications made and placed in production by EPA in fiscal 2003.

Limited Review of Financial Data Warehouse Performed

As part of the original scope of our review, we had planned to review the Financial Data Warehouse (FDW) system as well as IFMS. However, during our preliminary research phase, we found that management had not instituted a formal change control process over FDW, as specified in the Federal Information System Controls Audit Manual. We notified OCFO management of this weakness and, accordingly, did not pursue audit field work on FDW. In September 2003, the Comptroller took the first step toward developing a formal change control process by issuing a policy to establish an oversight structure for managing software changes to the FDW. We reviewed the policy and found that it does not contain sufficiently detailed procedures for the change control process being implemented. As such, we suggested that OCFO management expand upon the existing policy by developing and implementing a formal change control process with standardized procedures and techniques. We subsequently limited the scope of our work to permit OCFO time to implement the new policy and develop new procedures.

Prior Audit Coverage

The Office of Inspector General (OIG) noted issues related to internal software changes in a prior report, *Management of EPA's Technical Support Contract for Core Financial Systems Needs Improvement,* Report No. E1NMG6-15-0003-9100034, dated November 5, 1998. Among other things, the report noted that management needed to establish internal software change policies and procedures to provide management oversight and approval of core software development or enhancement projects, and discontinue direct supervision of contractor staff (i.e., personal services activities). Similar conditions noted in our current audit are discussed in Chapters 3 and 4.

Internal Controls

Our assessment of IFMS's software change control process and related security controls indicate EPA's core financial system is at risk for fraud, waste, and mismanagement. In planning and performing our audit, we limited our work to addressing operational and security controls associated with IFMS software modifications. During the period of our review, OCFO reported an internal control weakness due to the lack of a system security certification process for contractor personnel. Nevertheless, EPA's Administrator gave an unqualified statement of assurance in the Agency's Fiscal 2003 Integrity Act Report, based on OCFO's annual self-assessment of its internal management and financial control systems.

Compliance with Laws and Regulations

We identified noncompliances with portions of the Federal Acquisition Regulation related to contract management administration processes. (See Chapter 3.)

Chapter 2
Security Controls Inadequate to Protect Integrity of IFMS Software Libraries

We found a general breakdown of security controls that could undermine the integrity of IFMS software libraries and financial system data. Duties were not adequately segregated, individuals used an inappropriate ID or continued to have system access after no longer needing it, and contractor personnel were granted access to IFMS without a successful background security check. Despite many Federal and Agency policies, guidance, and procedures, numerous accountability and contractual issues contributed to poor management of the change control process and led to the general breakdown of security controls. This included OCFO not having a system for identifying employee responsibilities related to IFMS security, and management not performing a risk assessment of Endevor, the general support system used to control access to IFMS software libraries. As a result, there was a high risk that system programmers could make unauthorized changes to system software and data used for EPA's accounting and financial reporting.

System Supports IFMS Change Control Process

Endevor is an off-the-shelf general support system used to control the development, testing, and maintenance of IFMS libraries and software. EPA uses a contractor to administer Endevor but relies on EPA employees to perform associated Information Security Officer and RACF administration duties. Endevor provides controls over the movement of program code through the system life cycle management phases of IFMS. Endevor uses three basic "environments" to control libraries and software:

Environment	Description
Development	Contractor personnel use to develop software code and perform initial tests.
Quality Assurance	EPA module experts subsequently use for formal testing, such as systems testing.
Production	The software code is stored and executed from system software libraries.

These environments are further divided into multiple sequential life cycle stages. The environments and stages provide approval controls to ensure the system software advances in an orderly fashion through the systems life cycle stages and maintain access controls within stages. Software is migrated by Endevor sequentially from development to production environments. The IFMS Security

Plan states that Endevor's purpose is to ensure software code is approved by EPA personnel prior to moving the code, or revised code, into production. IFMS operations use Endevor to provide for data set and functional security by using RACF. A user is identified through a RACF-defined User-ID, and is authenticated through the password supplied with the User-ID at logon.

Numerous Federal regulations, industry best practices, and Agency policies and procedures provide benchmarks for evaluating EPA practices in dealing with security controls over the IFMS software change control process. This includes criteria from the Office of Management and Budget (OMB), Government Accountability Office (GAO), and NIST. The applicable criteria are listed in the following table, while further details are provided in Appendix A.

Applicable Criteria

- OMB Circular A-123, *Management Accountability and Control*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information*
- GAO *Federal Information System Controls Audit Manual*
- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- NIST SP 800-64, *Security Considerations in the Information Development Life Cycle*
- NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- EPA's *Information Security Manual*
- OCFO Policy Announcement 98-08, Amendment 1, *Procedures for On-line Access to EPA's Integrated Financial Management System*
- IFMS Security Plan
- EPA's *Application RACF Security Administrator's Guide*
- *Implementation Report for IFMS 5.1, Release 1 Using Endevor V3.6*

Improved Security Controls Needed

Logical Access Controls Over IFMS Software Inadequate

OCFO management had not established or instituted adequate logical access controls to protect the integrity of IFMS software libraries and data. We examined user access rights for 27 individuals, including 14 contractor personnel, who either: (1) possessed the ability to approve and move changes through Endevor, or (2) had access to Endevor through functionally-based RACF Groups. Specifically, we found the following:

> **Functions Not Segregated.** Sensitive change management functions had not been adequately segregated between contractor personnel to prevent any individual from controlling all critical stages of the process. We identified six EPA contractors who had the ability to both approve and move program code within each Endevor environment and from one environment to the next. Segregating sensitive duties would preclude the contractor from making unauthorized and perhaps untrackable changes.

Unneeded Access Remained. Five individuals no longer needing access to Endevor had not been removed from the RACF or RACF groups. This included a contractor who had not worked at EPA for several years. This Endevor contractor had a separate RACF User-ID and was assigned access rights through two of the five RACF groups. Further, management was not maintaining and using the RACF groups to control member access based on each group's functional roles, as intended by the 1995 Implementation Report for IFMS 5.1. Instead, individual users were assigned RACF User-IDs and given direct access rights within the various Endevor environments. This dual approach circumvented role-based access rights meant to enforce separation of duties, and allowed these individuals to bypass internal controls for modifying software code.

Sharing of User-IDs. Multiple contractor personnel routinely accessed Endevor environments using another individual's User-ID. Specifically, OCFO is allowing EPA contractors to use the User ID of OCFO's RACF Administrator to monitor the IFMS nightly cycle, which, subsequently, gives them access to IFMS production data. This presents an integrity risk because an "administrator" typically possesses advanced access rights.

Multiple IDs Used. Some OCFO employees possessed multiple RACF User-IDs, although OCFO management had not justified and obtained a formal waiver from EPA's National Technology Systems Division, as required by Agency procedures. Individuals possessing multiple IDs may loan out one or more of these IDs to other users, thus giving them inappropriate access rights and eliminating a verifiable audit trail.

Contractor Personnel Granted Access to IFMS Without Successful Security Screening

OCFO granted contractor staff sensitive access rights to IFMS production software and data even though OCFO had not requested or received assurance through the personnel security screening process that these individuals did not pose a significant risk to the integrity of the system. The contracts for Endevor and IFMS require that contractor staff submit background information to OCFO as a basis for initiating the security screening process. Of the at least 10 contractor staff assigned to the contracts, we found the following:

- Only three had acceptable "suitability" screenings. Further, for one of those three, the Office of Personnel Management had returned the request for screening stating EPA needed to adjudicate it; the Office of Environmental Information performed the adjudication, but OCFO had not been notified of the results.

- While the Office of Personnel Management had returned another two requests for screenings, OCFO had not revised and resubmitted them.

- OCFO had never initiated requests for contractor security screening for the remaining five contractor staff, including one for the individual serving in the sensitive role as an Endevor System Manager.

In addition, OCFO did not actively try to determine the status of requests that it had submitted for processing. Some of the requests had been pending a considerable length of time (sometimes more than a year), while OCFO continued to allow those contractors to perform duties that could have ultimately jeopardized the Agency's ability to produce accurate, complete, and reliable financial information and reports.

Endevor Logs Not Reviewed to Detect Problems or Assess Risk

OCFO personnel did not review Endevor audit logs, which are needed to give management assurance that only authorized change control activity is being conducted by recognized users. Endevor can produce a variety of reports that identify the User-ID associated with each system action, as well as when the action was performed. Neither OCFO's RACF Administrator nor the Information Security Officer requests these reports or review them periodically to detect problems or assess risk to the IFMS change control process.

Numerous Issues Contributed to Inadequate Management of Change Control Process

The primary factors contributing to the breakdown of security controls over OCFO's change management process for IFMS included the following:

- Management never performed a risk assessment for Endevor nor created a security plan to (1) describe the controls in place or planned to meet security requirements, or (2) delineate responsibilities and expected behavior for individuals who access the system. Although Endevor supported multiple OCFO systems, management had not recognized its significance to the financial system infrastructure.

- The Office of Administration and Resources Management's Security Management Division had not issued official policies and procedures to EPA's regional and program offices for defining the roles, responsibilities, and office interactions to ensure security screenings for non-Federal personnel. The OCFO Delivery Order Project Officer expressed confusion about his role and responsibilities. In April 2004, the Security Management Division issued a memo with interim guidance for handling screenings in a consistent, structured, and timely manner, but the Division is still working on additional guidance as well as training.

- The Statement of Work for the Endevor contract does not accurately reflect OCFO's current policy for screening contractor personnel who access IFMS. The Statement only requires a National Agency Check, although Amendment 1 of OCFO Policy 98-08 now indicates contractors should undergo a National Agency Check with Inquiries and Credit prior to being granted access to IFMS.

- OCFO has not established a system that clearly identifies key responsibilities or roles related to IFMS security and Endevor contract administration, and holds employees accountable for successful performance. In many cases, position descriptions do not accurately reflect an employee's current responsibilities or sufficiently detail significant duties related to Endevor contract management, information security oversight, or RACF administration. OCFO management acknowledged these concerns and, as a first step, is revising position descriptions for Financial Systems Staff.

- OCFO experienced considerable employee turnover because Financial Systems Staff employees either retired or were transferred to other divisions, and staff in key roles may not fully understand and execute assigned duties.

Security Weaknesses Threaten IFMS Data Integrity

The security control weaknesses noted significantly impact management's ability to place reliance on the integrity of data EPA uses for accounting and financial reporting purposes. In our opinion, the Agency faces the risk that unauthorized changes could be made to IFMS system software and data. The general breakdown of logical access controls could allow system programmers and analysts to surreptitiously modify, destroy, or change production system software and data. Unsafe practices are exacerbated by the facts that (1) OCFO is not using available audit logs to oversee change control activities, and (2) contractor staff are not receiving satisfactory security screenings before being granted sensitive access rights to IFMS software and data. These weaknesses could impede OCFO's ability to produce reliable data for financial managing and Congressional reporting purposes, and also could result in a disruption of IFMS operations.

Recommendations

We recommend that the Chief Financial Officer:

2.1 Perform a risk assessment of the Endevor system and, subsequently, develop a security plan for Endevor in accordance with NIST guidance, such as NIST Special Publication 800-18.

2.2 Update the Endevor Statement of Work to comply with current policies.

2.3 Remove access for all contractor personnel without a pending personnel security screening request or a final acceptable background check.

2.4 Establish a systematic process that will (1) clearly identify key responsibilities of roles related to IFMS security and Endevor contract administration; (2) ensure employees are adequately trained to perform assigned duties; and (3) hold employees accountable for successful performance of their roles by revising position descriptions and performance agreements.

We recommend the Acting Assistant Administrator for Administration and Resources Management:

2.5 Finalize the existing *Interim Procedures for Conducting Background Investigations* in a formal Agency-level policy.

2.6 Provide interim guidance on duties and responsibilities of coordinators for background investigations.

2.7 Provide training for Agency Delivery Order Project Officers and background security check coordinators for requesting background investigations of non-Federal personnel.

Agency Comments and OIG Evaluation

The Chief Financial Officer (CFO) and the Acting Assistant Administrator for OARM both provided responses to the security-related recommendations in our draft report. The CFO concurred on four recommendations and identified several actions to address reported weaknesses, such as updating the Endevor Statement of Work to comply with Agency policies. The Acting Assistant Administrator for OARM did not concur with the three recommendations concerning contractor background investigations.

The CFO agreed to perform a risk assessment of the Endevor system and to incorporate the results into IFMS's security plan. However, in our opinion, the best approach would be to create separate security plans for Endevor and IFMS. The CFO assumed operational responsibility for Endevor from EPA's Working Capital Fund and, as such, we believe that Endevor is a general support system and should not be combined with the security plan for the IFMS application. If the CFO still wants to prepare one, overarching security plan for the IFMS and Endevor systems, then it should be based on separate risk assessments of Endevor and IFMS. Moreover, the level of system information included in the overarching security plan should be sufficient to adequately (1) describe the controls in place or planned to meet security requirements, and (2) delineate responsibilities and expected behavior for individuals who access the system.

The CFO also agreed to establish a systematic process for securing IFMS, and listed several documents and actions taken that help employees understand their security responsibilities. However, OCFO needs to do more to ensure employees are held accountable for successfully performing their security roles. Therefore, we believe OCFO needs to (1) revise position descriptions for employees with IFMS security or Endevor contract administration responsibilities, and (2) update their performance standards to ensure accountability for these sensitive roles. Because these actions address security issues, the CFO should enter specific dates for these actions in the Agency's ASSERT system as a Plan of Action and Milestones.

The Acting Assistant Administrator for OARM did not agree to act on the report's recommendations, stating that background suitability screening of Federal contractors is not required by Federal or Agency-wide policy. Management stated that its interim procedures were sufficient to guide those program and regional offices that initiated background investigations due to internal requirements, and therefore, it did not need to finalize guidance or provide additional training to project officers or background security check coordinators. We disagree with management's decision to take no further action to formalize and strengthen the security screening process for contractor personnel. Both current EPA policy and NIST guidance strongly recommend that contractors have a comparable suitability screening to perform information technology work. Formalizing Agency-wide procedures would bring needed structure and consistency to the personnel screening process, and help clarify levels of risk and minimum screening requirements for non-Federal workers.

The Federal government is operating in a high risk environment and implementing wartime security operations, and we believe EPA and other agencies need to do more to screen non-Federal workers. Extra care needs to be taken to ensure non-Federal workers have acceptable, verifiable financial and lawful backgrounds before trusting them with sensitive access to data and systems, which could allow them access to privacy and credit card information or to disburse government funds. The Acting Assistant Administrator for OARM has been delegated the responsibility for maintaining an adequate Agency-level program for personnel security. We believe the current risk is not acceptable and management needs to react promptly and positively to the minimum corrective actions outlined above.

The Acting Assistant Administrator also noted that the term "security clearance" refers to investigations performed for individuals who need to access national security information, and, as such, we have modified the report to use the terms "background security check" or "personnel security screening."

Chapter 3
Contract Practices Over IFMS Software Modifications Need Improvement

OCFO did not manage the contract for IFMS software modifications in a manner that ensured the proper authorization, acceptance, and approval of all new and revised software. In particular, OCFO management did not properly use its Change Management System (CMS) to manage change activities for IFMS and provide technical direction to contractor staff, as required in the contract. Both the Federal Acquisition Regulation (FAR) and EPA policy outline acceptable procedures. Although we had previously identified contract management problems, OCFO continued to use contract practices that gave the appearance of an improper personal service relationship with the contractor. This close working relationship with the contractor does not provide acceptable contract management controls to protect the integrity of IFMS system software or data. A personal services relationship was clearly demonstrated when OCFO Financial Systems Staff orally instructed the contractor to bypass documented channels and correct erroneous transactions totaling over $222 million by entering negative debits and positive credits “directly” into IFMS.

CMS Contractually Required

CMS is a Lotus Notes application developed by EPA and required by the contract for managing IFMS change activities. OCFO’s Financial Systems Staff are required to use CMS to provide the contractor with technical direction for the tasks outlined in the Statement of Work. As such, an IFMS module expert should generate a work request – the primary means of prioritizing, identifying, and assigning work – within CMS to request contractor action. Subsequently, the contractor would use CMS to receive direction and provide deliverables for IFMS’s requirements and specifications. The contractor is only to accept work requests found in CMS or otherwise specifically approved by the Delivery Order Project Officer or Alternate Delivery Order Project Officer.

FAR Part 37.104 and EPA Order 1901.1A address personal services. FAR indicates an employer-employee relationship under a service contract occurs when, as a result of the contract’s terms or the manner of its administration during performance, contractor personnel are subject to the relatively continuous supervision and control of a Government officer or employee. Agencies are not to award personal services contracts unless specifically authorized by statute. EPA Order 1901.1A, “Use of Contractor Services to Avoid Improper Contracting Relationships,” states that technical direction shall be issued in writing from the authorized designee or, if provided orally, the technical direction must be confirmed in writing within 5 calendar days.

CMS Not Used to Manage Change Activities

EPA did not use CMS to ensure the proper authorization, acceptance, and approval of all new and revised IFMS software, as required by the contract. For example, the OCFO Financial Systems Staff did not use CMS to provide technical direction to the contractor staff and to document acceptance and approval of deliverables. Acceptance should signify that management has reviewed the deliverable and determined it meets contractual requirements; approval should denote the formal, contractual approval by the Delivery Order Project Officer. That Project Officer should then use the CMS approval as a basis for concurring with the contractor's requests for interim and final payments for the work. These controls ensure the contractor's work meets contractual expectations and is of a reasonable quality to warrant additional resources and proceeding to the next step.

We reviewed the CMS work requests for the seven software modifications implemented in August 2003, as the IFMS 5.1e10 Sub-Release, at a cost of $235,308. As of October 2003, for the 28 deliverables marked "required" in CMS, we found that:

- Fourteen (50%) had been marked received.
- Eight (29%) had been marked accepted by the module expert.
- Six (21%) had been marked approved by the Delivery Order Project Officer.

A breakdown by percentage for each of the modifications follows in the table:

Modification Number	Required Deliverables	Delivered	Accepted	Approved
1	3	100%	33%	33%
2	4	75%	75%	50%
3	5	60%	20%	20%
4	4	50%	50%	50%
5	8	25%	0%	0%
6	1	100%	100%	0%
7	3	0%	0%	0%
Total	**28**	**50%**	**29%**	**21%**

For 7 of the 28 deliverables, those initially marked as "required" in the CMS work request were later determined not to be necessary as a result of verbal discussions between the OCFO Financial Systems Staff and the contractor. Agreeing to decisions verbally without changing requirements in CMS treats contractors as employees and gives the appearance of personal services. In addition, because some required deliverables were not marked delivered, from a contractual standpoint it appeared that the Delivery Order Project Officer had concurred on payments for work not performed. Because other deliverables were never formally accepted or approved, it also appeared that the Delivery Order Project

Officer had concurred on payments for work that may not have met contractual requirements.

Position Descriptions Not Reflective of Employee Duties

We believe the above condition occurred, in part, because the current position descriptions for Financial Systems Staff personnel are outdated and not reflective of assigned Delivery Order Project Officer contracting responsibilities. OCFO employees' formal performance agreements and annual performance appraisals do not hold them accountable for satisfactory performance of contract management responsibilities. As such, OCFO management has not assessed how well these duties were carried out or whether they were performed in accordance with pertinent regulations, policies, and procedures. OCFO has acknowledged that existing Financial Systems Staff position descriptions are generic and lack details identifying employees' actual responsibilities, and are taking steps to revise them.

OCFO Did Not Address the Previously Noted Inadequacies

OCFO management did not address contract management problems previously noted in the OIG's 1998 report, but rather continued to use contract practices that give the appearance of an improper personal service relationship with the contractor. The 1998 report had recommended that management use CMS to document technical direction to contractor staff and provide an audit trail of all contract activity and contract deliverables. However, due to staff turnover, Financial Systems Staff management could not provide an explanation as to why corrective actions had not been taken.

Management Relationship Inadequate to Protect Integrity

OCFO Financial Systems Staff's close working relationship with the contractor for software development does not provide acceptable contract management controls to protect the integrity of IFMS system software or data. For example, the staff orally instructed the contractor to correct erroneous transactions totaling over $222 million by entering negative debits and positive credits "directly" into IFMS. Encouraging a contractor with application programming authority to process accounting entries is an inadequate segregation of duties and substantially increases IFMS's vulnerability to fraud, manipulation, and abuse. Specifically, the circumvention of internal controls increases the possibility that other unauthorized system software changes or modifications of accounting information could be made directly to the production version of IFMS.

Recommendations

We recommend that the Chief Financial Officer:

3.1 Continue Financial Systems Staff efforts to develop position descriptions that more accurately reflect the actual contracting roles and responsibilities for Financial Systems Staff employees, and explicitly incorporate contract management responsibilities in applicable performance agreements.

3.2 Instruct Financial Systems Staff to:

(a) Discontinue the practice of providing verbal technical direction to contractor staff (i.e., personal services activities).

(b) Document all meetings and other verbal directions to the contractor.

(c) Use CMS to document acceptance and approval of deliverables received from the contractor.

Agency Comments and OIG Evaluation

In responding to our draft report, the Chief Financial Officer concurred with both recommendations. In particular, management agreed to continue reviewing Financial Systems Staff employees' position descriptions to ensure they include appropriate contracting roles and responsibilities. This action, in conjunction with incorporating contract management responsibilities in applicable performance agreements, should fully satisfy the intent of the recommendation.

Chapter 4
Change Control Process Does Not Ensure Proper Authorization, Testing, and Approval

OCFO management has not instituted a formal, structured change control process for IFMS to ensure software program modifications are properly authorized, tested, and approved. EPA's security plan, which requires strong internal controls over the change control process to reduce the risk of unauthorized programs or modifications being implemented into the production environment, also serves as a basis for system security certification and accreditation. However, OCFO management did not implement formal change controls, as agreed to in a 1998 OIG report. Inadequate change controls over IFMS software modifications places the Agency at risk that the availability, confidentiality, and integrity of EPA’s accounting and financial reporting functions could be compromised.

Testing of Modifications Involves Various Stages

Testing of modifications or replacement software moves through a series of test stages. This includes:

- **Unit Testing:** Testing individual modules of program code.
- **Integration Testing:** Testing groups of modules that must work together.
- **System Testing:** Testing the entire system.

The contractor performs the unit testing by developing a unit test plan, documenting the results, and delivering them both to OCFO. Unit testing determines whether individual program modules perform to user specifications. OCFO module experts subsequently conduct the integration and system tests, to ensure that related system components and the system as a whole perform to specifications. At the completion of the testing phase, the system owner, who has developmental and execution authority for the system, recommends implementation; the sponsor, who is authorized by the system owner to initiate system development, approves the implementation of the modified or replacement software.

GAO, OMB, and NIST provide criteria and best practices for formal internal control procedures. In December 2003, EPA issued an Interim Agency System Life Cycle Management Policy (Interim EPA Order 2100.4), which, along with the rescinded directive (EPA Directive 2100, Chapter 17), assigns system managers the responsibility for managing their system’s life cycle process and products in compliance with Agency and Federal policy. The Interim Order requires EPA management to review and document its approval or disapproval in a decision document at each of the five system life cycle phases before the system may advance to the next phase. Further, the IFMS Security Plan, dated

September 2002, states that a formal change control process should be in place, and that all changes to the application software should be tested and approved prior to being placed into production. All changes are to be documented. Further details on criteria are in Appendix A.

Change Control Process Inadequate

OCFO Not Following Agency Process for Authorizing Projects

OCFO management did not adhere to the Agency's process, as established by EPA's new Interim EPA Order 2100.4 as well as the directive it replaced, for a decision paper to authorize and establish the project for the IFMS sub-release. The new interim order also requires a decision paper to authorize the start of a project, and expands upon this requirement to include a formal authorization at the end of each system life cycle phase. Audit work disclosed that EPA's Financial Systems Staff formally notified OCFO management once it had determined which enhancements should be included in a planned system sub-release. However, we could not find any formal OCFO concurrence for the 2003 sub-release information provided by the staff to the Comptroller. Based on available evidence, it appears that OCFO management did not formally authorize the proposed software modifications prior to development, testing, and implementation.

Inadequate Control Process for Testing and Approval

OCFO management has not instituted a formal change control process for testing changes made to IFMS system software. Further, the existing informal process is not adequate to ensure all new and revised software is properly tested and approved. While Financial Systems Staff had conducted *systems* testing for all seven software modifications implemented as part of the August 2003 IFMS sub-release, the staff had only done the *integration* testing for 43 percent of the modifications (three of seven). Both tests play important roles to ensure the modified software will operate as intended without negatively impacting the other system operations or degrading system performance. However, a module expert stated that the Financial Systems Staff considers system testing to be more important than integration testing; hence, they maintain detailed documentation for system testing but not integration testing results. This module expert also indicated the staff has plans to eliminate integration testing and only perform system testing in the future, but we believe that would be inappropriate.

IFMS's Security Plan recognizes the importance of both integrated and system testing, and requires that they be performed and documented as part of the change management process because the system is mission-critical. OCFO is required to develop and document a test plan to ensure the right combination of functions are being tested. The results of the test must also be documented, because they serve as a means for comparing actual test results and those anticipated in the test plan.

These documents provide the basis for management to certify that controls are adequate for operational purposes. The following table shows the lack of integration and system test plans and corresponding documented results for each of the 2003 sub-release software modifications.

Modification	Integration Test Plan	Integration Test Results	System Test Plan	System Test Results
1	Yes	Yes	Yes	Yes
2	No	No	Yes	Yes
3	Yes	Yes	Yes	Yes
4	No	No	Yes	Yes
5	Yes	Yes	Yes	Yes
6	No	No	No	Yes
7	No	No	Yes	Yes
	3	3	6	7
Percent	43%	43%	86%	100%

Furthermore, in those instances where the Financial Systems Staff conducted integration and system tests, it did not maintain an evidentiary trail to support satisfactory supervisory reviews and management approvals of the test plans and corresponding test results. Financial Systems Staff personnel indicated that testing results are discussed verbally with their team leader and acceptance is verbally communicated by the team leader to the module expert; no formal, written approval is provided.

Based on our review of testing documentation, we believe the Chief for Financial Systems did not have an adequate basis for recommending implementation of the 2003 August IFMS sub-release. Relying on the informal, verbal acceptance and approval processes for system and integration testing, the Financial Systems Staff sent a formal memorandum to the Director for Financial Management to request concurrence on implementation of the sub-release. The Director formally responded with an approval to proceed with installation. In our opinion, the Chief for Financial Systems did not have adequate evidence to support the decision.

IFMS Certification and Accreditation Not Based on a Structured and Disciplined Control Process

IFMS was authorized to operate in 2002, based on a security risk assessment and security plan process that did not strongly emphasize the importance of a structured, disciplined approach to managing, controlling, and documenting system changes. Subsequent to the 2002 authorization, NIST published new guidelines for Security Certification and Accreditation of Federal information systems, formally recognizing configuration and management control as an essential element for maintaining a system's security accreditation (i.e., formal authorization to operate). Although this newer requirement did not exist when IFMS was formally authorized to operate, it is a current and compelling reason for management to establish and enforce a structured process for documenting information system changes and assessing the impact of the those changes on the security of the system.

OCFO Did Not Address Previously Identified Control Weaknesses

OCFO management did not implement formal change controls, as recommended in the prior 1998 OIG report. In response to previously noted weaknesses, OCFO had agreed to establish internal software change control policies and procedures that would provide management oversight and approval of core system software development and enhancement projects. Due to staff turnover, Financial Systems Staff management could not provide an explanation as to why actions had not been taken to correct continuing contract management problems.

According to Interim EPA Order 2100.4, it is EPA's goal that all major application systems will be developed using a methodology equivalent to at least the Software Engineering Institute's Capability Maturity Model Level 3. For IFMS to meet that goal, the change control process for IFMS system software would need to be reengineered so that it is documented, standardized, and integrated into a standard software management control process for OCFO.

Uncontrolled System Software Changes Could Compromise Availability, Confidentiality, and Integrity of IFMS Data

Uncontrolled change controls over IFMS software modifications places the Agency at risk that the availability, confidentiality, and integrity of EPA's accounting and financial reporting functions could be compromised. System software changes should be carefully controlled and approved since relatively minor program changes, if done incorrectly, can compromise or have a significant negative impact on overall data reliability. Moreover, a structured and disciplined process for managing, controlling, and documenting changes is an essential element for maintaining system accreditation. The absence of such a vital control process could negatively impact the Authorizing Official's decision to continue system operations, because this lapse of controls could pose an unacceptable level of risk to Agency operations, assets, or individuals.

If management does not develop and implement structured controls to ensure software modifications are properly authorized, tested, and approved, program changes could result in erroneous processing, weakened access controls, or weakened system edits. Furthermore, without an orderly, disciplined process for testing and approving new and modified programs prior to their implementation, management cannot ensure that (1) IFMS programs will operate as intended,

(2) no unauthorized software changes have been incorporated into pending releases, or (3) an adequate basis exists for providing required system security certification and accreditation.

Recommendations

We recommend that the Chief Financial Officer:

4.1 Identify an OMB-reportable Plan of Action and Milestones to establish and implement a new, structured change control process over IFMS using a methodology that meets the specifications published in EPA's interim system life cycle management policy and procedures.

4.2 Within 90 days, reauthorize and accredit IFMS in accordance with NIST 800-37, assessing the security risks in place at that point of time. If the risk to Agency operations, assets, or individuals cannot be addressed within this timeframe, then consider issuing an Interim Authorization to Operate, in accordance with NIST guidance, until such time as the new policy and procedures are fully implemented.

Agency Comments and OIG Evaluation

In responding to our draft report, the Chief Financial Officer concurred with both recommendations. The CFO noted that a new CMS system is currently under development and that management is studying NIST guidance to determine what action is required for re-authorizing and re-accrediting IFMS. We are concerned with the focus of the CFO's response, because replacing CMS alone will not fully address the intent of our recommendations. CMS is only used to manage the "contract" for IFMS's change management activities. This is only a portion of the IFMS change control process, which also includes management's initial authorization of projects, integrated and systems testing, the system owner's formal recommendation for implementation, and the final approval to implement the modified or replacement software into the production environment. As such, to fully address the intent of our recommendations, the CFO will also need to develop, document, and implement a structured change control process for IFMS that complies with EPA's interim system life cycle management policy and procedures, and incorporates the new CMS.

Applicable Criteria

Numerous Federal regulations, industry best practices, and Agency policies and procedures establish the baseline for evaluating OCFO's practices in securing and processing changes to IFMS. Details follow.

- **Appendix III to OMB Circular A-130, Security of Federal Automated Information Resources, dated November 2000.** This defines adequate security as "security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information." This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability. Appendix III also indicates that agencies should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST. Also, Appendix III discusses the need for a security plan and a risk assessment for Federal agencies' general support systems.

- **OMB Circular A-123, Management Accountability and Control, dated June 1995.** The Circular establishes specific management control standards requiring separation of duties and supervision, and access to and accountability of resources.

- **The Chief Financial Officers Act of 1990.** This Act requires financial management systems to comply with internal control standards.

- **Federal Financial Management Improvement Act, dated September 1996.** This Act identifies internal controls as an integral part of improving financial management systems.

- **Federal Information System Controls Audit Manual (FISCAM), dated January 1999.** This GAO manual states that a formal change control process includes instituting policies, written procedures, and techniques that help ensure all programs and program modifications are properly authorized, tested, and approved. Also, this manual represents government-wide information technology best practices, such as for logical access controls and segregation of duties issues for software change controls.

- **NIST.** NIST represents Federal guidance covering security controls over general support systems and applications. Several NIST Special Publications (SPs) apply:

  NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, dated May 2004. This stresses the importance of adequate configuration management and control, recognizing it as an essential element for maintaining a system's security accreditation. Security certification and accreditation is part of a dynamic, ongoing risk management process, which culminates in a formal authorization to operate an information system based on the state of security at a specific point in time. NIST emphasizes that the inevitable changes to an information system (including software) and the potential impact those changes may have on agency operations, agency assets, or individuals, requires an orderly and disciplined approach to managing, controlling, and documenting changes so as to ensure an ongoing assessment of their impact on system security.

NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dated September 1996. This gives recommendations on how proper segregation of duties should be established, and on how appropriate logical access controls should be implemented.

NIST SP 800-64, Security Considerations in the Information Development Life Cycle, dated October 2003. This discusses issues and gives recommendations for personnel security screenings.

NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, dated December 1998. This provides detailed guidance on creating security plans for general support systems.

- **GAO's Standards for Internal Control in the Federal Government**, **dated November 1999.** The Standards require management to document, test, and approve modifications to software before placing them into production.

- **EPA Order 2100.4, Interim Agency System Life Cycle Management Policy, dated December 2003**. EPA issued this Interim Order and rescinded Chapter 17 of EPA Directive 2100, which nevertheless was in effect during the 2003 IFMS sub-release process. The new policy applies to all information systems developed, enhanced, or maintained by or for EPA, including applications and general support systems. OCFO's change control procedures and practices are based on the Agency's system development life cycle concepts. EPA's System Life Cycle Management Policy consists of five phases. One of the phases is the Operation and Maintenance phase, which requires OCFO to operate and maintain IFMS software using a configuration management process. Periodic risk assessments, testing, certification, and reauthorization must be conducted during this phase. The new policy states that systems must be developed in a rigorous manner that lessens and manages risk.

  The Interim Order further establishes important roles and responsibilities for controlling changes to system software during the operation and maintenance phase. This policy, as well as the rescinded Chapter 17, assigns system managers the responsibility for managing their system's life cycle process and products in compliance with Agency and Federal policy. While Chapter 17 assigned responsibility for formally approving system enhancements to the system sponsor, the Interim Order assigns this responsibility to the system owner. In particular, it notes that the System Owner is responsible for ensuring (1) adherence to the System Life Cycle Management Policy, and (2) that all management and security controls are in place and operational. In addition, it defines the IFMS System Owner's responsibilities, which include recommending the implementation of changes to system software. The Interim Order also states the IFMS System Manager controls daily operations. Further, the System Sponsor must concur with advancement of the software modifications, replacements, or enhancements to each life cycle phase. In addition, the Senior Information Resources

Management Official is the Authorizing Official that approves the security plan authorizing operations.

Further, the Interim Order requires EPA management to review and document its approval or disapproval in a decision document at each of the five system life cycle phases before the system may advance to the next phase. The accompanying Interim Agency System Life Cycle Procedures further define the Implementation Phase, which requires testing and a written authorization to process prior to beginning operations. Testing the system ensures that it works as specified in the requirements and design specifications, and that it meets applicable standards of performance, reliability, integrity, and security.

- **EPA's Information Security Manual (ISM), dated December 1999**. The Manual sets forth requirements and provides guidance for securing Agency information resources in accordance with EPA and Federal security policies and mandates. Specifically, the Manual lists requirements for personnel security screenings, logical access controls, and establishing proper segregation of duties.

- **OCFO Policy Announcement 98-08, Amendment 1, Procedures for On-line Access to EPA's Integrated Financial Management System (IFMS), dated March 2002**. This identifies requirements for personnel security screenings. Specifically, it requires that background screenings include, at least, a successful National Agency Check with Inquiries and Credit before giving contractor personnel access to IFMS.

- **IFMS Security Plan, dated September 2002.** The IFMS Security Plan states that a formal change control process should be in place and that all changes to the application software should be tested and approved prior to being placed into production. The Plan also states that the process for testing revisions to the software should include EPA performing testing first in an integrated test environment and then in a more comprehensive system test environment. Further, the Plan states that all changes to the application software should be documented, including integrated test plans, system test plans, and test results. Finally, The IFMS Security Plan identifies local and Agency provisions for the IFMS Security Administrator to use for maintaining proper segregation of duties, and establishing appropriate logical access controls.

- **EPA's Application RACF Security Administrator's Guide, dated February 1996.** The Guide provides procedural guidance required for EPA program offices to perform RACF administration. The Guide outlines requirements for RACF User-ID administration. For instance, the Guide prohibits the sharing of User-IDs and individuals from owning more than one User-ID, unless the National Technology Services Division receives a justification from the system owner and approves the exception.

- **The Implementation Report for IFMS 5.1, Release 1 Using Endevor V3.6, dated February 1995.** The Report identifies EPA's responsibility and procedures for maintaining RACF groups associated with Endevor.

Office of the Chief Financial Officer Response to Draft Report

MEMORANDUM

DATE: July 23, 2004

SUBJECT: OIG Audit Report: EPA Needs to Improve Change Controls for
Integrated Financial Management System
2003-000909

FROM: Charles E. Johnson, Chief Financial Officer /s/
Office of the Chief Financial Officer

TO: Patricia H. Hill, Director
Business Systems Audits

Thank you for the opportunity to respond to the findings and recommendations made in the draft report entitled, "EPA Needs to Improve Change Controls for Integrated Financial Management System." Attached is our response to the specific audit findings and recommendations made in the report. Comments from the Office of Administration and Resources Management were provided under separate cover.

We agree with the OIG emphasis on the importance of change controls. However, we disagree with the OIG assertion that there is a general breakdown of security controls that could undermine the integrity of our financial system and data. Our office exerts significant effort to ensure that security controls provide reasonable assurance, limit access to authorized individuals, and properly integrate software modifications. To this end, we continually initiate actions that will enhance our existing controls. For example, a recently developed automated annual security recertification system, grounded in the concepts of least privilege and proper separation of duties, is being used to update access rights, privileges, roles for Integrated Financial Management System and the Financial Data Warehouse users. Actions are also underway to replace the antiquated Change Management System. Additionally, key change control roles and responsibilities are clearly defined and employed by our trained systems experts.

We acknowledge that there is always room for improvement in any process and welcome your continued evaluation of our efforts.

If you have any questions concerning this response, please contact Lorna McAllister, Acting Director, Office of Financial Management at 202-564-4905 or Juanita Galbreath, Staff Director, Financial Systems Staff at 202-564-1560.

Attachment

cc: Mike Ryan

RESPONSE to DRAFT AUDIT of EPA's CHANGE CONTROL for
THE INTEGRATED FINANCIAL MANAGEMENT SYSTEM

FINDINGS AND RECOMMENDATIONS

2 – Security Controls Inadequate to Protect Integrity of IFMS Software Libraries

We recommend that the Chief Financial Officer (OCFO):

2.1 Perform a risk assessment of the Endeavor system and, subsequently, develop a security plan for Endeavor in accordance with NIST guidance, such as NIST Special Publication 800-18.

***FSS Response: C**oncur*

Endeavor is not a system. Rather, it is a software tool used to automate, control and monitor application development and maintenance. It maintains complete source code audit trials and provides source code library management functions. Access to Endeavor menus and options is controlled by Resource Access Control Facility (RACF).

Endeavor does not meet the NIST 800-18 definition of a "major application" or "general support system." that requires a security plan. Endeavor:

- *is not* mission critical;
- *is not* reviewed under the Agency's annual IT Investment review process as a Major Application "Full CPIC";
- *does not* have high confidentiality requirements, i.e., contain confidential business information, trade secrets, privacy information or any other highly confidential information;
- *does not* have high availability requirements;
- *does* have high integrity requirements.

However, to further ensure financial systems integrity, we will include endeavor in the IFMS security plan and risk assessment.

2.2 Update the Endeavor Statement of Work to comply with current policies.

FSS Response: Concur

We have reviewed the Statement of Work (SOW) for the IAG and found that it does have a requirement for a National Agency Check (NAC). We will request that GSA update the SOW to require at a minimum a National Agency Check with Inquiries and Credit (NACIC).

Note: Our contractor currently has a security clearance through another Federal agency for which she performs additional work.

2.3 Remove access for all contractor personnel without a pending personnel security screening request or a final acceptable clearance.

FSS Response: Concur

We have reviewed the personnel security information of each contractor and in accordance with EPA Information Security Manual (ISM), Directive 2195, A-1, section 10, taken the appropriate action.

2.4 Establish a systematic process that will:

(1) Clearly identify key responsibilities of roles related to IFMS security and Endevor contract administration; (2) ensure employees are adequately trained to perform assigned duties; and (3) hold employees accountable for successful performance of their roles.

FSS Response: Concur

Current OCFO, FSS guidance, policies, assignment matrix's and employee performance plans clearly identify key roles and responsibilities and enforce accountability. Additionally, FSS employees receive continual training to better prepare them to successfully fulfill their responsibilities.

- The IFMS Security Features Users Guide (SFUG) clearly identifies roles and responsibilities and provides the information that a user needs to enter IFMS and start working within its security constraints, and it explains the user's role in maintaining the security of the system.
- The IFMS Procedures for Online Access provides procedures for controlling on-line access.
- The entire Financial Systems Staff received 8 hours of IFMS Security Training in October 2003, and 16 hours IFMS refresher training in December of 2003. In addition, internal ongoing training is provided by each staff subject matter expert to other staff members.

Additional applicable documentation available to FSS and IFMS end-users is:

- PA 98-08, FSS Policies and Procedures for On-line Access to the EPA's Integrated Financial Management System (IFMS), September 1998 available at http://intranet.epa.gov/ocfo/policies/policy/pa98-08a.pdf
- IFMS Computer Based Instruction (CBT) available at http://intranet.epa.gov/ocfo/systems/fsb/ifms.htm#cbt

2.5 Finalize the existing Interim Procedures for Conducting Background Investigations in a formal Agency-Level policy. Addressed by OARM

2.6 Provide interim guidance on duties and responsibilities of coordinators for background investigations. Addressed by OARM

2.7 Provide training for Agency Delivery Order Project Officers and security clearance coordinators for requesting background investigations of non-Federal personnel. Addressed by OARM

3 – Contracting Practices Over IFMS Software Modifications Need Improvement

3.1 Continue Financial Systems Staff efforts to develop Position Descriptions that more accurately reflects the actual contracting roles and responsibilities for Financial System Staff employees, and explicitly incorporate contract management responsibilities in applicable performance agreements.

FSS Response: Concur

The FSS Director will continue to review staff position descriptions to include the appropriate contracting roles and responsibilities.

3.2 Instruct Financial Systems Staff to:
(a) Discontinue the practice of providing verbal technical direction to contractor staff (i.e., personal services activities). (b) Document all meetings and other verbal directions to the contractor. (c) Use CMS to document acceptance and approval of deliverables received from the contractor.

FSS Response: Concur

The Director of FSS has instructed the responsible parties to (1) document all meetings with and directions provided to the contractor and (2) use CMS to document acceptance and approval of all deliverables from the contractor. The contractor has been notified in writing to not accept any verbal instructions from Financial Systems Staff.

4 – Contracting Practices Over IFMS Software Modifications Need Improvement

4.1 Identify an OMB-reportable Plan of Action and Milestones (POAM) to establish and implement a new, structured change control process over IFMS using a methodology that meets the specifications published in EPA's interim system life cycle management policy and procedures.

FSS Response: Concur

A new Change Management System is currently under development. The POAM will include Policies and Standard Operating Procedures.

4.2 Reauthorize and accredit IFMS in accordance with NIST 800-37 if the new change control process cannot be implemented within the next 90 days.

FSS Response: Concur

Due to fiscal year-end close-out and IFMS sub-release requirements, we do not expect to implement the new CMS in the next 90 days. We are currently studying the new NIST guidance to determine what action is required.

Appendix C

Office of Administration and Resources Management Response to Draft Report

July 21, 2004

MEMORANDUM

SUBJECT: Response to Draft Audit Report: EPA Needs to Improve Change Controls for Integrated Financial Management System

FROM: David J. O'Connor, Acting Assistant Administrator /S/

TO: Patricia H. Hill, Director
Business System Audits

I appreciate the opportunity to review the subject audit report and to provide this response to your recommendations directed to OARM. Our Security Management Division is very supportive of Agency efforts to improve security of its financial management systems and has endeavored to assist OCFO in their background investigations of contractor employees.

I believe the use of the term "security clearance" in connection with your audit is inappropriate because clearances are required only when access to national security information is needed which is not applicable for the tasks identified in your audit cases. Furthermore, even if such clearances were needed, the Department of Defense, not EPA, has the authority to grant them.

The substantive issue in your draft report that is relevant to OARM is "suitability" background investigations which are currently mandated only for federal employees to determine if they are "fit for service." No federal or EPA-wide policy currently requires suitability screening of contractors. A few offices, including OCFO, have elected to establish such a policy and we provide support for the processing and adjudication of these investigations. However, because of the limited nature of these, we do not believe that our interim procedures need to be formalized or expanded Agency-wide at this time.

Attached is a detailed response to your audit recommendations from Rich Lemley, Director of the Office of Administrative Services. Please direct any further inquiries regarding this response to Rich at 564-8400.

cc: Rich Lemley
Wes Carpenter
Sandy Womack-Butler

Attachment

July 14, 2004

MEMORANDUM

SUBJECT: Response to Draft Audit Recommendations Regarding Interim Procedures for Conducting Background Investigations on Non-Federal EPA Workers

FROM: Rich Lemley, Director /S/
Office of Administrative Services

TO: Patricia H. Hill, Director
Business System Audits

I am pleased to provide this response to the recommendations contained in the subject report pertaining to our Security Management Division. I hope you will find this information useful and request that you direct any further questions to me at 564-8400.

As you know, background suitability screening of federal contractors is not required by any federal or Agency-wide policy. However, because a few EPA program offices have elected to screen some contractors, in early 2004, our Security Management Division issued an internal memo regarding "Interim Procedures for Conducting Background Investigations on Non-Federal EPA Employees." This document states that it applies only to those programs and regions with internal policies in place requiring background investigations and it clarifies the process for initiating them through the Office of Personnel Management (OPM). Because the Agency has not established a mandatory EPA-wide formal policy regarding these investigations, we do not believe that the interim procedures should be finalized into such a document as you recommend in 2.5 below.

2.5 Finalize the existing *Interim Procedures for Conducting Background Investigations* in a formal Agency-level policy.

Response: No federal or Agency-wide policy exists for suitability screening of contractors so the interim procedures should remain limited to those EPA programs and regions that voluntarily have elected to conduct such investigations.

2.6 Provide interim guidance on duties and responsibilities of coordinators for background investigations.

Response: The Security Management Division has already provided guidance on procedures to follow for initiating suitability background investigations of contractors through OPM. The duties and responsibilities of program and regional coordinators should be established by their respective offices, if needed.

2.7 Provide training for Agency Delivery Order Project Officers and security clearance coordinators for requesting background investigations of non-Federal personnel.

Response: Currently, very few EPA personnel are involved in requesting background investigations of non-federal personnel and the Security Management Division has worked with them on an individual basis to explain the procedures. We do not believe that formal training is required at this time.

APR 26 2004

MEMORANDUM

SUBJECT: Interim Procedures for Conducting Background Investigations on Non-Federal EPA Workers

FROM: Wesley J. Carpenter, Chief */s/*
Security Management Division

TO: All Program and Regional Security Representatives

These procedures are directed at those EPA Programs and Regions with internal policies in place requiring background investigations for non-federal workers performed through the Office of Personnel Management (OPM). For those Programs and Regions without existing internal policies, these procedures are not mandatory.

The process for non-federal background investigations at EPA is set forth in a six step process. Of those six steps, only step one and step six require involvement of the Program or Regional Office. All steps require participation and collaboration with OARM's Security Management Division (SMD), Personnel Security Branch. The six step process outlined below will improve communications and the overall awareness of personnel security within the Agency.

NOTE: A new standard is currently being developed to establish minimum personnel security suitability requirements for non federal employees supporting EPA. Once finalized, it will supplement the SMD's existing procedures. In the interim, based on previous SMD guidance, Programs and Regions should use the formal process set out below.

Step 1: The Programs and Regions must complete and submit the required paperwork to the Personnel Security Branch.

- The Program or Regional Contracting Officer Representative (COR) must complete and submit a cover memo and contractor security documents to the Personnel Security Branch to initiate the process

  < Cover memorandum, including:

  ÷ Name and telephone number of COR;

  ÷ Name and telephone number of points of contact for obtaining additional information and notification of adjudication determination, if different from the COR;

  ÷ Contract number;

÷ Name of contractor(s) for whom security paperwork is provided;

÷ Identification of type of background investigation requested; and

÷ Funding information.

< Non-federal security documents, including:

÷ SF-85P, Questionnaire for Public Trust Positions; or

÷ SF-85, Questionnaire for Non-Sensitive Positions;

÷ Two FD-258, Federal Bureau of Investigation fingerprint charts;

÷ SF-86A, Continuation Sheet for Questionnaires, when applicable; and

÷ Credit Release Authorization Form (for investigations requiring a credit check: MBI, LBI or NACI with Credit).

NOTE: The SF-85 PS Questionnaire is not required and should not be used. In addition, Part I of the SF-85P or SF 85 form will be completed by the Personnel Security Branch; the Programs and Regions should not complete it.

- The cover memorandum and contractor security documents should be hand-delivered or mailed to the Personnel Security Branch at:

< US EPA
Attention: Personnel Security Branch
1200 Pennsylvania Ave., NW
Mail Code 3206M, East Building - Room B414
Washington, DC 20460

Step 2: The Personnel Security Branch will enter the information into its database, file copies of the information, and review the contents of the case papers.

Step 3: The Personnel Security Branch will initiate the investigation through OPM.

Step 4: OPM will conduct the investigation and forward the completed investigation to the Personnel Security Branch for adjudication. On average, this process takes 2 to 8 months to complete.

Step 5: The Personnel Security Branch will favorably or unfavorably adjudicate the case and provide the results to the Program or Regional COR.

Step 6: The Program or Regional COR will review the adjudicative results and take action based on the findings and recommendations. OPM is notified of final adjudicative action.

Questions regarding these procedures should be directed to Kelly Glazier, Chief, Personnel Security Branch at 202-564-0351.

Appendix D

Distribution

Chief Financial Officer (2710A)
Acting Assistant Administrator for Administration and Resources Management (3101A)
Acting Director, Office of Financial Management (2733R)
Director, Office of Administrative Services (3201A)
Director, Technical Information Security Staff (2831T)
Audit Coordinator, OCFO (2710A)
Audit Coordinator, OARM (3102A)
Audit Coordinator, OEI (2812T)
Agency Follow-up Official (2710A)
Agency Follow-up Coordinator (2724A)
Associate Administrator for Congressional and Intergovernmental Relations (1301A)
Associate Administrator for Public Affairs (1701A)
Inspector General (2410T)