United States General Accounting Office

GAO

Report to the Secretary of the Treasury

October 1999

FINANCIAL MANAGEMENT SERVICE

Significant Weaknesses in Computer Controls

GAO

Accountability * Integrity * Reliability

GAO/AIMD-00-4

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-283555

October 4, 1999

The Honorable Lawrence H. Summers
The Secretary of the Treasury

Dear Mr. Secretary:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 1998 financial statements, we reviewed the general and application computer controls over key financial systems maintained and operated by the Department of the Treasury's Financial Management Service (FMS). On August 31, 1999, we issued a "Limited Official Use" report to you detailing the results of our review. This excerpted version of the report for public release summarizes the weaknesses we identified and the recommendations we made.

This report discusses the results of our fiscal year 1998 tests of the effectiveness of general and application controls that support key FMS automated financial systems and our follow-up on the status of FMS' corrective actions to address weaknesses identified in our fiscal year 1997 audit.[1] These systems, some of which are operated and maintained by contractors and the Federal Reserve Banks (FRB), are critical to FMS' mission of serving as the government's financial manager, central disburser, collections agent, and reporter of financial information. We have issued a separate report to the Board of Governors of the Federal Reserve System on the results of our testing of the general and application controls over key FMS systems that the FRBs maintain and operate.

As discussed in this report, we identified computer control weaknesses at FMS and its contractor data centers that place its financial systems at significant risk of unauthorized disclosure and modification of sensitive data and programs, misuse or damage to computer resources, or disruption of critical operations. Also, the pervasiveness of these weaknesses places billions of dollars of payments and collections at risk of fraud.

[1] *Financial Management Service: Areas for Improvement in Computer Controls* (GAO/AIMD-99-10, October 20, 1998).

While performing our work, we communicated detailed information regarding our findings to FMS management. This report provides an overall assessment and summary of FMS' computer control weaknesses and recommendations to you as the agency head.

Results in Brief

The pervasive weaknesses we identified in FMS' computer controls at each of its data centers during our fiscal year 1998 audit renders FMS' overall security control environment ineffective in identifying, deterring, and responding to computer control weaknesses in a timely manner. Our follow-up on the status of FMS' corrective actions to address weaknesses identified in our fiscal year 1997 audit found that FMS had only corrected or mitigated the risks associated with 24 of 72 computer control weaknesses discussed in our "Limited Official Use" report issued on July 31, 1998.

During the fiscal year 1998 audit, we found new general computer control weaknesses in entitywide security planning and management, access controls, system software, and application software development and change controls. We also identified weaknesses in the authorization controls over all six of the key FMS financial applications we reviewed. In addition, we identified an accuracy control weakness over one of the six key FMS financial applications and a completeness control weakness over another one of the six key FMS financial applications.

Because of the weaknesses in computer controls that we identified, including the lack of an effective entitywide security planning and management program, billions of dollars of payments and collections are at significant risk of loss or fraud, vast amounts of sensitive data are at risk of inappropriate disclosure, and critical computer-based operations are vulnerable to serious disruptions. Accordingly, as reported for fiscal year 1997, we continue to consider FMS' computer control problems a material weakness.[2] FMS has also recognized the serious nature of these problems and has reported these matters in its Federal Managers' Financial Integrity Act (FMFIA) report for fiscal year 1998.

[2]A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material to the financial statements may occur and not be detected promptly by employees in the normal course of performing their duties.

Background

FMS is the government's financial manager, central disburser, and collections agency as well as its accountant and reporter of financial information. For fiscal year 1998, the U.S. government disbursed over $1.6 trillion primarily for Social Security and veterans benefit payments, IRS tax refunds, federal employee salaries, and vendor billings. With several exceptions (the largest being the Department of Defense), FMS makes disbursements for most federal agencies.

FMS is also responsible for administering the federal government's collections system. In fiscal year 1998, the government collected over $1.7 trillion from sources such as individual and corporate income tax deposits, customs duties, loan repayments, fines, and proceeds from leases. FMS maintains a network of about 11,000 financial institutions to help collect these revenues.

In addition, FMS oversees the federal government's central accounting and reporting systems used to reconcile and keep track of the federal government's assets and liabilities. Financial and budget execution information from these central systems is used by FMS to publish financial reports that are available for use by the Congress, the Office of Management and Budget, other federal agencies, and others who make financial decisions on behalf of the U.S. government.

FMS maintains a wide array of financial and information systems to help it process and reconcile monies disbursed and collected by the various government agencies. Multiple banking, collection, and disbursement systems are also used to process agency transactions, record relevant data, transfer funds to/from the Treasury, and facilitate the reconciliation of these transactions.

FMS has seven data centers and utilizes data processing services at several contractors and the FRBs, which help FMS carry out its financial management responsibilities.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the computer controls over FMS' key financial management systems and to determine the status of the computer control weaknesses identified in our fiscal year 1997 audit. We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years, each data center and key application is subjected to a full-scope review that includes testing in all of the computer control areas defined in our *Federal Information System Controls Audit Manual* (FISCAM).[3] During the interim years, we focus our testing on the FISCAM areas that we have determined to be at greater risk for computer control weaknesses. See appendix I for the scope and methodology of our fiscal year 1998 review at each of the selected data centers[4] and for the key applications.

During the course of our work, we communicated our findings to FMS management who informed us of the corrective actions they planned or had taken to address the weaknesses we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

We performed our work from August 1998 through February 1999. Our work was performed in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Department of the Treasury. The FMS Commissioner's comments are discussed in the "Agency Comments" section of this report.

[3] *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6, January 1999).

[4] The data centers we reviewed consisted of data centers at both FMS and its contractors.

FMS' Entitywide Security Planning and Management Program Is Not Effective

As we discussed in our prior year report, the overriding reason that computer control problems exist at FMS is because it does not have an effective entitywide computer security planning and management program. An entitywide program for security planning and management is the foundation of an entity's security control structure and should establish a framework for continual (1) risk assessments, (2) development and implementation of effective security procedures, and (3) monitoring and evaluation of the effectiveness of security procedures. A well-designed entitywide security planning and management program helps to ensure that security controls are adequate, properly implemented, applied consistently across the entity, and responsibilities for security are clearly understood. Our May 1998 best practices guide [5] on information security management practices at leading nonfederal organizations found that organizations successfully managed their information security risks through an ongoing cycle of risk management activities. An effective program would include guidance and procedures for assessing risks, establishing appropriate policies and related controls, and monitoring and evaluating the effectiveness of established controls.

One of the most fundamental elements of an effective entitywide security planning and management program is a current and comprehensive entitywide security policy to communicate security management plans, standards, regulations, or guidelines. An entitywide security policy provides the foundation for a computer security program and helps management ensure that computer controls are working and are reliable, established policies and procedures are followed, identified deficiencies are timely corrected, and errors or fraudulent transactions are timely detected. FMS' security policies and related procedures have not been formally updated since 1991. FMS has drafted a "Project Manager's Security Handbook" to provide guidance for the implementation and documentation of its information technology security controls. However, the handbook has not been approved and implemented. Based on the results of our audits over the past 2 years, FMS' entitywide security control structure has failed to address many of the significant risks associated with its current computing environment.

[5] *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

Specifically, FMS' approach to security planning and management lacked

- adequate site-specific written policies and procedures to ensure security administration roles and responsibilities are clearly defined and communicated and that procedures are comprehensive and appropriate for the particular computing environment;
- management enforcement of established security policies and procedures, such as completing background investigations and security violation monitoring and follow-up; and
- adequate training of the data center security administrators to ensure security techniques and parameters are properly administered and applied.

These weaknesses in security planning and management expose FMS to the risk that other general control weaknesses could occur and not be detected in a timely manner to prevent unnecessary losses or disruptions.

Serious General Computer Control Weaknesses Place FMS Systems and Data at Significant Risk

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. They include an entitywide security planning and management program, access controls, system software controls, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security planning and management program is in place, (2) protect data, files, and programs from unauthorized access, modification, and destruction, (3) limit and monitor access to programs and files that control computer hardware and secure applications, (4) prevent the introduction of unauthorized changes to systems and applications software, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

Our follow-up on the status of FMS' corrective actions to address weaknesses identified in our fiscal year 1997 audit found that three of the seven data centers had made little or no progress in correcting or mitigating the risks associated with the general computer control weaknesses identified at those data centers. FMS officials stated that older operating systems were being replaced with newer operating systems at two of its data centers. Thus, FMS has elected not to take corrective

actions on selected weaknesses at these data centers until the planned migrations are completed. In addition, FMS stated that it is moving one of its key applications to a distributed environment and anticipates this migration to be completed in 2001. Further, FMS expects that these migrations will facilitate the implementation of more effective controls in the future.

However, many of the weaknesses we identified in our fiscal year 1997 audit at these data centers will not be corrected by moving to new operating environments. For example, service continuity plans still need to be fully developed and tested for its new systems covering all aspects of their mission-critical business functions. More importantly, during system migrations, FMS' exposure to serious disruption of operations, disclosure of sensitive programs and data, or intrusions by hackers or malicious internal users is increased by the following factors:

- the seriousness and pervasiveness of the problems as they exist today,
- the absence of essential compensating controls to mitigate the serious risks, and
- experienced delays and the possibility of future delays in the implementation of the new systems.

As a result, we are repeating those prior year findings related to these data centers that have not been corrected as well as reaffirming the related recommendations discussed in our "Limited Official Use" version of this report.

Our fiscal year 1998 review of FMS' general computer controls identified serious new general control weaknesses in access controls, system software, and application software development and change controls.

Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security control measures involve the use of computer hardware and security software programs to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific

systems, programs, and files they need to conduct their work and to prevent unauthorized users from gaining access to computing resources.

Physical security controls include locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

Our review of FMS' access controls identified a number of weaknesses at all of the sites we visited. These weaknesses, many of which were included in our prior year report, included data centers that (1) had weak network security configurations, (2) granted excessive and powerful systems privileges to users who did not need such access, (3) did not manage the administration of passwords and user IDs effectively, (4) were not applying security system parameters so as to provide optimum security or appropriate segregation of duties, and (5) were not adequately monitoring and controlling access to multiple processing environments. For example:

- Messages and data sent and received by the mainframe applications through the network were not sufficiently controlled, increasing the risk that malicious users could gain unauthorized access to computer resources or disrupt operations.
- All users, including programmers and computer operators at one data center, had the capability to read sensitive production data, such as security-setting tables and tax payment information, increasing the risk that sensitive information may be disclosed to unauthorized individuals.
- Certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.
- Security software system parameters were not set consistently at the data centers or at industry-recommended settings to provide a more secure environment, thereby significantly increasing the risk that unauthorized system functions could be executed without detection.
- The remote access to the multiple processing environments at two data centers was not sufficiently controlled, thereby providing inadequate protection from unauthorized access by intruders.

Due to the sensitive nature of the internal network control weaknesses we identified, these issues are described in the separate "Limited Official Use" report issued to you on August 31, 1999.

In addition, physical security controls at four of the seven sites we visited were not sufficient to control physical access to these centers. In particular, as we also found in our prior year audit, production staff, terminated employees, vendors, and other individuals without justified business or job-related purposes had unrestricted access to computer facilities, equipment, and tape libraries. In addition, we found at one of these sites that controls and accountability over backup tape inventories were not adequate.

The risks created by these access control weaknesses were heightened because FMS was not adequately managing and monitoring user access activities. Program managers and security personnel did not consistently monitor and evaluate user access rights, security violations, and software security settings at all seven sites visited. These access control weaknesses also place FMS at risk that unauthorized activities, such as corruption of financial data, disclosure of sensitive data, or introduction of malicious programs or unauthorized modifications of software, will go undetected.

System Software

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software includes operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

At several of the seven data centers visited, the software library listings did not agree with the corresponding volume locations or indexes on the systems or contained obsolete or unneeded library members. Such system software control weaknesses increase the risk that standard security software could be bypassed to obtain access to restricted system functions. In addition, the use of such library members could cause unexpected operating results.

Application Software Development and Change Controls

Controls over the design, development, and modification of application software help to ensure that all programs and program modifications are properly authorized, tested, and approved. Such controls also help prevent security features from being inadvertently or deliberately turned off and processing irregularities or malicious code from being introduced.

We found application software development and change control procedure weaknesses at six of the seven FMS sites we visited. As we reported in the prior year, a significant weakness at most of the sites we visited was that policies and procedures over system design, development, and modification were not established, were inadequate, or were simply not being followed. Specifically,

- procedures for making changes to application and system software were not always followed, such as (1) obtaining written authorizations prior to making the changes, (2) developing written test plans, (3) independent testing of changes, or (4) authorizing the migration of application software changes from the test environment to production;
- programmers at one data center compile their own source code, which was not independently recompiled to ensure that only authorized changes made to programs were moved into production; and
- adequate documentation was not consistently maintained to provide evidence of compliance with established application software development and change control policies and procedures.

Without adequate control over application software development and change control procedures, FMS runs a greater risk that software supporting its operations will not (1) produce reliable data, (2) execute transactions in accordance with applicable laws, regulations, and management policies, or (3) effectively meet operational needs.

Segregation of Duties

Another key control for safeguarding programs and data is to ensure that duties and responsibilities for authorizing, processing, recording, and reviewing data, as well as initiating, modifying, migrating, and testing of programs, are separated to reduce the risk that errors or fraud will occur and go undetected. Duties that should be appropriately segregated include applications and system programming and responsibilities for computer operations, security, and quality assurance. Policies outlining the supervision and assignment of responsibilities to groups and related individuals should be documented, communicated, and enforced.

We found that the FMS data centers had taken actions to partially resolve segregation of duty weaknesses we reported in the prior year. However, at two of the seven sites visited, programmers continued to have access rights to production data. Duties that are not appropriately segregated significantly increase the risk that improper program changes could be

made or computer data and systems resources could be altered, damaged, or destroyed.

Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

Because it is not cost-effective to provide the same level of continuity for all operations, it is important that organizations analyze relevant data and operations to determine which are the most critical and what resources are needed to recover and support them. As discussed in our May 1998 best practices guide, the criticality and sensitivity of various data and operations should be determined and prioritized based on an overall risk assessment of the entity's operations. Factors to be considered include the importance and sensitivity of the data and other organizational assets handled or protected by the individual operations and the cost of not restoring data or operations promptly.

In reviewing FMS' service continuity controls, we found that our prior year recommendations had been partially addressed. However, FMS' newly developed central service continuity plan did not prioritize the manner in which key business processes should be brought up in the event of an emergency. In addition, as we reported in the prior year, four of the seven data centers visited had not developed and tested service continuity plans covering all aspects of their mission-critical business functions. Consequently, these FMS data centers are still at risk that in the event of an emergency or disaster, data center personnel may not be prepared to effectively prioritize recovery activities, integrate recovery steps in an effective manner, or fully recover systems.

FMFIA Reporting

FMFIA requires ongoing evaluations of the internal control and accounting systems that protect federal programs against fraud, waste, abuse, and mismanagement. It further requires that the heads of federal agencies report annually to the President and the Congress on the condition of these controls and systems and on their actions to correct the weaknesses identified.

During the course of our work, we communicated our general computer control findings to FMS management. As a result, FMS reported its general computer control problems as a material weakness to the Department of the Treasury. The Department of the Treasury reported in its fiscal year 1998 Accountability Report that FMS, along with other Treasury components, had a material weakness in general computer controls designed to safeguard data, protect computer application programs, prevent system software from unauthorized access, and ensure continued computer operations.

FMS' Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs, which are used to perform a certain type of work, such as generating interest payments or recording transactions in a general ledger. In an effective general control environment, application controls help to further ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

Authorization Controls

Like general access controls, authorization controls for specific applications should be established to (1) ensure individual accountability and proper segregation of duties, (2) ensure only authorized transactions are entered into the application and processed by the computer, (3) limit the processing privileges of individuals, and (4) prevent and detect inappropriate or unauthorized activities.

Our review of FMS' authorization controls found a number of weaknesses over each of the six key financial applications we tested. These weaknesses included

- incomplete, missing, or unapproved user application request forms;
- inappropriate access to application functions and privileges that were not required by the users' job responsibilities and that in some instances also created an inadequate segregation of duties;

- terminated or dormant user IDs were not adequately controlled;
- users sharing IDs or being assigned multiple IDs without a functional requirement;
- security reports not being consistently monitored or followed up on; and
- application passwords not being properly managed.

The authorization control weaknesses described above increase the risk of unauthorized activities such as inappropriate processing of transactions, unauthorized access or disclosure of sensitive data, corruption of financial data, or a disruption of operations not being prevented.

Accuracy Controls

The recording of valid and accurate data into application systems is essential to an effective system that produces reliable results. Accuracy controls include (1) well-designed data entry processes, (2) data validation and editing to identify erroneous data, (3) reporting, investigating, and correcting erroneous data, and (4) review and reconciliation of output.

We found one accuracy control weakness over one key FMS financial application involving transmittal reports that did not reconcile to each other and certain of those reports contained outdated and inaccurate data. Reports that do not reflect valid and accurate data increase the risk that unreliable financial results will be produced by the application.

Completeness Controls

Completeness controls are designed to ensure that all transactions are processed and missing transactions are identified. Common completeness controls include the use of record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data.

Our review of completeness controls over one key FMS financial application found that there were no automated record counts and control totals to ensure that data transferred from one application to another application were complete.

FRB Computer Controls Can Be Improved

Our follow-up work found that the FRBs had corrected or mitigated the risks associated with 14 of the 20 vulnerabilities that were identified in our prior year report and that work is in progress to address the remaining vulnerabilities. While we found that the FRBs had implemented effective

general and application controls over key FMS systems that the FRBs maintain and operate, our fiscal year 1998 audit procedures identified certain new vulnerabilities in general controls that do not pose significant risks to the FMS financial systems, but nonetheless warrant FRB management's attention and action. These include vulnerabilities in general controls over (1) access to data, programs, and computing resources, (2) system software, and (3) service continuity. We also found vulnerabilities in authorization controls over two key FMS financial applications and completeness controls over one key FMS financial application. We are providing details of these matters in a separate report to the Board of Governors of the Federal Reserve System along with our recommendations for improvement. FRB management has informed us that the FRBs have taken or plan to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

Conclusion

FMS has not instituted the appropriate preventive measures through its entitywide security planning and management program to further reduce its exposure to the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations. Also, the pervasiveness of the computer control weaknesses—both old and new weaknesses—at FMS and its contractor data centers place billions of dollars of payments and collections at risk of fraud. The severity of these risks magnifies as FMS expands its networked environment through the migration of its financial applications from mainframes to distributed environments. Thus, as FMS provides users greater and easier access to larger amounts of data and system resources, well-designed and effective general and application controls are essential if FMS' operations and computer resources are to be properly protected. It will take a significant and sustained commitment by FMS' management to fully address its serious computer control weaknesses, including establishing an effective entitywide computer security planning and management program.

Recommendations

In our August 31, 1999, "Limited Official Use" version of this report, we reaffirmed our prior year recommendation that you direct the Commissioner of the Financial Management Service, along with the Assistant Commissioner for Information Resources, to establish an effective entitywide security planning and management program.

In addition, we recommended that you direct the Commissioner of the Financial Management Service, along with the Assistant Commissioner for Information Resources, to correct each individual weakness that we identified and address each of the specific recommendations that were summarized in that report.

Further, we recommended that you direct the Commissioner of the Financial Management Service, along with the Assistant Commissioner for Information Resources, to work with the FRBs to implement corrective actions to resolve the computer control vulnerabilities related to FMS systems supported by the FRBs that we identified and communicated to the FRBs.

Agency Comments

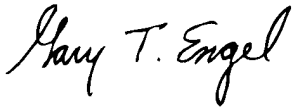
In commenting on a draft of this report, FMS stated that it recognizes that there continue to be serious weaknesses in computer controls. FMS stated that actions are currently in progress for all of the outstanding weaknesses and indicated that additional actions had been taken since the end of our fieldwork to correct or mitigate many of the weaknesses identified in our fiscal year 1997 audit. FMS has also stated that converting its payment processing systems to newer systems would facilitate the implementation of more effective controls in the future. As we discussed in our report, it is important that FMS ensure that the computer controls over the new operating systems are effectively implemented. We will follow up on these matters during our audit of the federal government's fiscal year 1999 financial statements. In addition to its written comments, the staff of FMS provided technical comments, which have been incorporated as appropriate.

We are sending copies of this report to Senator Robert C. Byrd, Senator Ben Nighthorse Campbell, Senator Pete V. Domenici, Senator Byron L. Dorgan, Senator Frank R. Lautenberg, Senator Joseph Lieberman, Senator Daniel Patrick Moynihan, Senator William V. Roth, Jr., Senator Ted Stevens, and Senator Fred Thompson, and to Representative Bill Archer, Representative Dan Burton, Representative Stephen Horn, Representative Steny H. Hoyer, Representative John R. Kasich, Representative Jim Kolbe, Representative David R. Obey, Representative Charles B. Rangel, Representative John M. Spratt, Jr., Representative Jim Turner, Representative C.W. Bill Young, and Representative Henry A. Waxman in their capacities as Chairmen or Ranking Minority Members of Senate or House Committees and Subcommittees. We are also sending copies of this report to Mr. Richard L. Gregg, Commissioner, Financial Management Service; the Honorable

Jeffrey Rush, Jr., Inspector General, Department of the Treasury; the Honorable Jacob Lew, Director, Office of Management and Budget; and other agency officials. Copies will be made available to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-3406. Key contributors to this assignment were Paula M. Rascona, Christine A. Robertson, and Gregory C. Wilshusen.

Sincerely yours,



Gary T. Engel
Associate Director
Governmentwide Accounting and
Financial Management Issues

Appendix I

Scope and Methodology

We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each data center and key application is subjected to a full-scope review that includes testing in all of the computer control areas defined in FISCAM. During the interim years, we focus our testing on the FISCAM areas that we have determined to be at greater risk for computer control weaknesses.

The scope of our work for fiscal year 1998 included follow-up on weaknesses identified in our fiscal year 1997 audit and reviews at FMS data centers[1] consisting of

- a focused review at one of the FMS data centers of the three general controls areas intended to
  - ensure that an adequate computer security planning and management program is in place;
  - protect data, files, and programs from unauthorized access, modification, and destruction; and
  - limit and monitor access to programs and files that control computer hardware and secure applications;
- a focused review at another two of the FMS data centers of the two general controls areas intended to
  - protect data, files, and programs from unauthorized access, modification, and destruction and
  - limit and monitor access to programs and files that control computer hardware and secure applications; and
- a focused review at a fourth FMS data center of the general controls intended to limit and monitor access to programs and files that control computer hardware and secure applications.

We limited our work at another three FMS data centers to a follow-up review of the status of weaknesses identified in our fiscal year 1997 audit.

To evaluate these general controls, we identified and reviewed FMS' information system general control policies and procedures, conducted tests and observed controls in operation, and held discussions with officials at selected FMS data centers to determine whether controls were in place, adequately designed, and operating effectively. We performed penetration testing at four FMS data centers. Our penetration testing was expanded this year to also include internal penetration testing procedures.

[1]The data centers we reviewed consisted of data centers at both FMS and its contractors.

Through our internal and external penetration testing, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of certain FMS officials.

We performed full-scope application controls reviews of five key FMS applications to determine whether the applications are designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and timely;
- data are properly processed by the computer and files are updated correctly;
- erroneous data are captured, reported, investigated, and corrected; and
- files and reports generated by the application represent transactions that actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

The scope of our work over certain key modules of a sixth key FMS application focused on the following two application control areas to determine whether the applications are designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) prevent and detect inappropriate or unauthorized activities and
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and timely.

Because the FRBs are integral to the operations of FMS, we followed up on the status of the FRB's corrective actions to address vulnerabilities identified in our fiscal year 1997 audit. We assessed general controls over FMS systems that the FRBs maintain and operate. We also evaluated application controls over three key FMS financial applications maintained and operated by the FRBs.

To assist in our evaluation and testing of computer controls, we contracted with the independent public accounting firm PricewaterhouseCoopers LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related working papers to ensure that the resulting findings were adequately supported.

During the course of our work, we communicated our findings to FMS management who informed us that the FMS has taken or plans to take corrective actions to address the weaknesses we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

We performed our work from August 1998 through February 1999. Our work was performed in accordance with generally accepted government auditing standards.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER