United States General Accounting Office

GAO

Report to the Secretary of the Treasury

October 1998

FINANCIAL MANAGEMENT SERVICE

Areas for Improvement in Computer Controls

GAO/AIMD-99-10

GAO

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

Accounting and Information
Management Division

B-280887

October 20, 1998

The Honorable Robert E. Rubin
The Secretary of the Treasury

Dear Mr. Secretary:

We recently reported on our audit of the U.S. government's consolidated financial statements for fiscal year 1997 (GAO/AIMD-98-127, March 31, 1998). Our report on the U.S. government's internal controls described widespread computer control weaknesses that place enormous amounts of federal assets at risk of fraud and misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

Our audit, done pursuant to the Chief Financial Officers Act of 1990, as expanded by the Government Management Reform Act of 1994, included testing the effectiveness of general computer controls over key financial systems used by the Financial Management Service (FMS). These financial systems, some of which are maintained and operated 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.

On July 31, 1998, we issued a "Limited Official Use" report detailing weaknesses in FMS' general computer controls. This version of the excerpted report for public release provides a general summary of the weaknesses we identified and the recommendations we made.

General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They are intended to (1) protect data, files, and programs from unauthorized access, modification, and destruction, (2) prevent the introduction of unauthorized changes to systems and applications software, (3) ensure that system software development and maintenance, applications software development and maintenance, computer operations, security, and quality assurance functions are performed by different people, (4) ensure recovery of computer processing operations in case of a disaster or other unexpected interruption, and (5) ensure that an adequate computer security planning and management program is in place.

Results in Brief

General computer control weaknesses at FMS and its contractor data centers place the data maintained in its financial systems at significant risk of unauthorized modification, disclosure, loss, or impairment. Because of the large volume of transactions, the significance of the related amounts involved, and the number of weaknesses identified at the FMS data centers visited, we consider FMS' general computer control problems a material weakness.[1] The general control weaknesses we found included (1) inappropriate access to computer programs, data, and equipment, (2) inadequate segregation of duties, (3) improper application software development and change control procedures, and (4) incomplete or untested service continuity and contingency plans.

General computer control weaknesses place billions of dollars of payments and collections at risk of fraud. These weaknesses existed primarily because FMS does not have an effective entitywide computer security planning and management program to ensure that (1) computer controls are working and are reliable, (2) established policies and procedures are followed, (3) identified deficiencies are timely corrected, and (4) errors or fraudulent transactions are timely detected.

FMS has already corrected some of the weaknesses that we identified, such as changing user access profiles or system security options to restrict users to only those system resources needed to perform their jobs and enhancing application software development and change control procedures to ensure that only authorized and approved changes or modifications are made to the system. Although FMS management is continuing to correct weaknesses we identified, FMS cannot ensure on an ongoing basis that weaknesses will be timely detected and corrected until it has an effective entitywide security management program. Such a program, if implemented effectively across the organization, would go a long way in helping FMS to identify and promptly address its computer control weaknesses.

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 1997, FMS reported processing over 850 million disbursements totaling over $1 trillion for a wide variety of expenses, including Social Security and veterans benefits payments, IRS tax refunds,

[1]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.

federal employee salaries, and vendor billings. With several exceptions (the largest being the Department of Defense), FMS makes disbursements for all federal agencies.

FMS is also responsible for administering the world's largest collections system. Each year, the government collects over $1.5 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 18,000 financial institutions to help collect these revenues.

In addition, FMS oversees the federal government's central accounting and reporting systems 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 used 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, capture relevant data, transfer funds to/from the Treasury, and facilitate the reconciliation of these transactions.

FMS has data centers at six regional financial centers that are responsible for issuing paper check and electronic funds transfer payments. In addition, FMS relies on a network of contractors and FRBs to help carry out its financial management responsibilities.

The FMS Commissioner and Assistant Commissioner, Information Resources, are responsible for overseeing the development, implementation, and operation of the organizationwide information data processing systems, including the establishment of appropriate general computer controls. Individual system users, such as FMS financial operations and federal finance staff located in Washington, D.C., and the six regional financial centers, civilian federal agencies, FRBs, contractor staff, and commercial bank staff are also responsible for overseeing and ensuring the security of individual systems and information under their purview.

Objectives, Scope, and Methodology

Our objectives were to evaluate and report on the general computer controls over key financial systems maintained and operated by FMS and its contractors. These systems process collections and disbursements and provide financial and budget reports for the federal government.

Specifically, we evaluated general controls intended to

- protect data, files, programs, and equipment from unauthorized access, modification, and destruction;
- provide adequate segregation of (1) duties involving applications and system programmers and (2) responsibilities for computer operations, security, and quality assurance;
- prevent the introduction of unauthorized changes to systems and applications software;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure that an effective entitywide computer security planning and management program is in place.

To evaluate general controls, we identified and reviewed FMS' general computer control policies and procedures; conducted tests and observations of controls in operation; and held discussions with staff at the locations visited to determine whether the general controls were in place, adequately designed, and operating effectively. In addition, we attempted to obtain access to sensitive data and programs from within and outside the organization. These attempts were performed with the knowledge and cooperation of FMS officials.

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

During the course of our work, we communicated our interim detailed findings and recommended corrective actions to FMS management and its contractors who informed us of the corrective actions they planned to take or had taken to address the findings we identified. We performed additional work to assess the status of any corrective actions taken as of September 30, 1997. These results were also communicated to FMS.

We performed our work at FMS data centers located throughout the United States. We performed our work from March 1997 through January 1998 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Secretary of the Treasury or his designee. On September 24, 1998, the Assistant Fiscal Assistant Secretary provided us with oral comments. These comments are summarized in the "Agency Comments" section of this report.

Information in FMS' Systems Is at Significant Risk Because of Serious General Control Weaknesses

Our review of FMS' general computer controls identified numerous weaknesses that place FMS' financial systems at significant risk of unauthorized access, improper modification, loss, and disclosure. These weaknesses include

- inappropriate access to computer programs, data, and equipment;
- inadequate segregation of duties;
- improper application and systems software development and change control procedures; and
- incomplete or untested service continuity and contingency plans.

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, loss, and disclosure. Such controls include logical, system software, and physical controls.

Logical controls include user identifications (ID), passwords, or other identifiers and security software programs. Logical 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. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

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 espionage, sabotage, damage, and theft.

Our review of FMS' access controls identified a number of weaknesses at all of the sites we visited. Those weaknesses included data centers that (1) granted excessive and powerful systems privileges to users who did

not need such access, (2) did not manage the administration of passwords and user IDs effectively, (3) were not applying security system parameters so as to provide optimum security or appropriate segregation of duties, and (4) were not monitoring and controlling dial-in access to local area networks and the mainframe environments. For example:

- System operators were given unneeded access to program utility products used to perform maintenance to operating system code, production source code, and production data, exposing the data center to the risk of unauthorized changes to system software or data.
- The user IDs of terminated employees were not removed from the system on the dates of termination and one showed activity after that date, thus increasing the risk of unauthorized access to system resources.
- A substantial number of agency user IDs have not been used for an extended period, increasing the risk that intruders could use these accounts to gain unauthorized access to system resources.
- All users, including programmers and computer operators at one data center, have 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.

In addition, physical security controls at four of the sites we visited were not sufficient to control physical access to these centers. In particular, we found that 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.

The risks created by these control weaknesses were heightened because FMS was not adequately managing and monitoring user access activities. In some instances, program managers and security personnel did not periodically monitor and evaluate user access rights, security violations, and software security settings. FMS is also 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.

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 assignment of these responsibilities to groups and related individuals should be documented, communicated, and enforced.

We found segregation of duty weaknesses at three of the seven sites we visited. These weaknesses primarily involved

- programmers (both systems and applications programmers) who served as backup computer operations staff and had access rights to production data and
- systems programmers who served as backup security officers and could alter security functions and access system resources.

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. Because FMS' activities involve extremely large volumes of monetary transactions, erroneous or fraudulent program or data changes could potentially result in significant financial losses to the federal government.

Application Software Development and Change Control Procedures

Controls over the design, development, and modification of system 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 that we visited. 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 system software did not require (1) written authorizations prior to making the changes, (2) written test plans, (3) independent testing of changes, or (4) authorization to migrate system software changes from the test environment to production;
- programmers compile their own source code, which was not independently recompiled to ensure that only authorized changes made to programs are moved into production; and

- adequate documentation was not maintained to provide evidence of compliance with application 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.

Service Continuity and Contingency Planning

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) contingency plans for recovering critical operations should interruptions occur.

A contingency 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 and employees should be trained in and familiar with its use.

In reviewing FMS' service continuity and contingency planning, we found that

- FMS does not have a centralized service continuity and contingency plan that includes its multiple contractors and regional financial centers and
- four of the data centers visited had not developed and tested service continuity and contingency plans covering all aspects of their mission-critical functions.

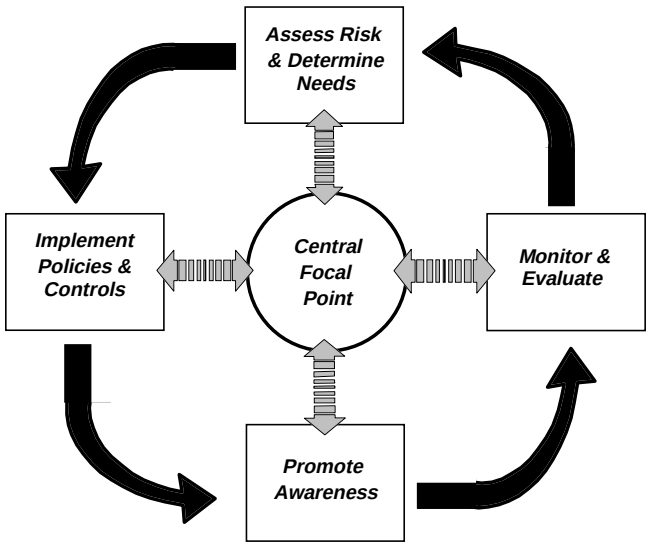
Weaknesses in FMS' service continuity and contingency planning provide FMS with little assurance that during a crisis (1) the cost of recovery efforts or the reestablishment of operations at a remote location will be kept to a minimum, (2) financial data will not be lost, (3) transactions will be processed accurately and correctly, and (4) complete and accurate financial or management information will be readily available.

Entitywide Computer Security Planning and Management Program Is Not Effective

The overriding reason general control problems existed at FMS was because it does not have an effective entitywide computer security planning and management program to oversee organizationwide security efforts, ensure that adequate controls are established, and ensure that computer security receives adequate attention.

Our study[2] of security management practices of eight nonfederal organizations found that these organizations successfully managed their information security risks through an ongoing cycle of risk management activities. As shown in figure 1, each of these activities is linked in a cycle to help ensure that business risks are continually monitored, policies and procedures are regularly updated, and controls are in effect.

Figure 1: Risk Management Cycle



The risk management cycle begins with an assessment of risks and a determination of needs. This assessment includes selecting cost-effective policies and related controls. Once policies and controls are selected, they must be implemented. The policies and controls, as well as the risks that prompted their adoption, must next be communicated to those responsible for complying with them. Finally, and perhaps most important, there must be procedures for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can

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

take appropriate corrective action. In addition, our study found that a strong central security management focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

FMS' approach to computer security planning and management lacked

- adequate written policies and procedures for security administration;
- routine management reviews of (1) security exception and violation reports, (2) password maintenance and the related timely removal of terminated employee or dormant user IDs, and (3) user access verification and recertification processes; and
- management enforcement of established security policies and procedures.

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.

FRB Computer Controls Can Be Improved

Because FRBs are integral to the operations of FMS, we assessed general controls over FMS financial systems and application controls over four key FMS financial applications maintained and operated by FRBs. Overall, we found these controls were effective. However, we found several vulnerabilities in general and application controls that require FRB management's attention and action. These include vulnerabilities in general controls involving (1) access to systems, programs, and data, including unauthorized external access, and (2) service continuity and contingency planning. We also found a vulnerability in access controls over one of the applications. We are providing the details of these matters in a separate report to the Board of Governors of the Federal Reserve System along with our recommendation for improvements. FRB management has informed us that 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 federal government's fiscal year 1998 consolidated financial statements.

Year 2000 Date Conversion

The Year 2000 date conversion poses a challenge for many organizations, including federal agencies. The Year 2000 problem is rooted in the way dates are recorded and calculated in many computer systems. For the past several decades, systems have typically used two digits to represent the year in order to conserve electronic data storage and reduce operating

costs. With this two-digit format, however, the year 2000 is indistinguishable from the year 1900. As a result, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999.

Because FMS' core business processes involve information systems, it is critical that FMS ensure that its mission-critical and key financial management systems are Year 2000 compliant. FMS officials have stated that they are continuing to make progress in assessing and converting systems for Year 2000 transition. A review of such actions was not included in the scope of our work performed to evaluate and test FMS computer controls. We are working with the Congress and the executive branch to monitor the progress being made by federal agencies and identify specific recommendations for resolving the Year 2000 problem. In connection with this work, we will review FMS' actions.

Conclusion

FMS does not have effective general controls in place to protect critical computer systems, programs, and data from inadvertent or deliberate misuse, fraudulent use, alteration, or destruction. Because of the large volume of transactions, the significance of the related amounts involved, and the number of weaknesses identified at the FMS data centers we visited, we consider FMS' general computer control problems a material weakness. Moreover, FMS has not instituted a proactive approach for identifying, deterring, and responding to computer control weaknesses in a timely manner.

Recommendations

To improve weaknesses in general controls cited in our July 31, 1998, "Limited Official Use" version of this report, we recommended that you direct the Commissioner of the Financial Management Service, along with the FMS Information Resources Assistant Commissioner, to take the following actions.

- Correct the individual weaknesses that we identified and communicated to FMS management during our testing, which were summarized in the "Limited Official Use" report. Assign responsibility and accountability for correcting each weakness to designated individuals. These individuals should report to the Commissioner on the status of all weaknesses, including actions taken to correct them.
- Work with other appropriate assistant commissioners to ensure that an effective entitywide security planning and management program is in

place. This program should include the following elements: (1) a strong central security management focal point to ensure that major elements of a risk management program are carried out and to provide a communications link among organizational units, (2) periodic risk assessments and needs determinations, (3) policy and controls implementation, (4) promotion of computer control awareness through training and other attention-getting techniques, and (5) evaluation and monitoring of policy and control effectiveness.

- Work with the Federal Reserve Banks to implement the corrective actions that we identified and communicated to them during our testing related to FMS systems that FRBs support.
- Identify the computer control weaknesses discussed in the "Limited Official Use" report as a material weakness in FMS' fiscal year 1998 Federal Managers' Financial Integrity Act report and subsequent reports until they are corrected.

Agency Comments

Treasury agreed with our findings and recommendations. Treasury stated that FMS has planned or already taken actions to correct many of the individual weaknesses that we identified and communicated to FMS management during our testing, which were summarized in the "Limited Official Use" report. We will evaluate FMS' efforts to address these matters during our audit of the federal government's fiscal year 1998 consolidated financial statements.

We are sending copies of this report to the Commissioner of the Financial Management Service; the Director of the Office of Management and Budget; the Chairman of the House Committee on Ways and Means; and the Chairmen and Ranking Minority Members of the Senate Committee on Appropriations and its Subcommittee on Treasury and General Government; Senate Committee on Finance; Senate Committee on Governmental Affairs; Senate Committee on the Budget; Subcommittee on Treasury, Postal Service, and General Government, House Committee on Appropriations; House Committee on Government Reform and Oversight and its Subcommittee on Government Management, Information and Technology; and House Committee on the Budget. We will send copies to others upon request.

This work was performed under the direction of Gary T. Engel, Associate Director, Governmentwide Accounting and Financial Management Issues,

who can be reached at (202) 512-3406. Other major contributors to this report are listed in appendix I.

Sincerely yours,

Gene L. Dodaro
Assistant Comptroller General

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Christine A. Robertson, Assistant Director
Paula M. Rascona, Audit Manager
Gregory C. Wilshusen, Assistant Director—Technical Advisor

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested