United States General Accounting Office

GAO

Report to the Secretary of the Treasury

January 2002

FINANCIAL MANAGEMENT SERVICE

Significant Weaknesses in Computer Controls Continue

GAO-02-317

Contents

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

January 31, 2002

The Honorable Paul H. O'Neill
The Secretary of the Treasury

Dear Mr. Secretary:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 2000 financial statements,[1] 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) as of September 30, 2000. These systems, some of which are operated and maintained by contractors and the Federal Reserve Banks (FRB), are critical to FMS's mission of serving as the government's financial manager, central disburser, collections agent, and reporter of financial information. On December 14, 2001, we issued a Limited Official Use report detailing the results of our review. This excerpted version of the report for public release summarizes (1) the significant weaknesses we identified and recommendations we made and (2) our follow-up on previously reported weaknesses.

The computer control weaknesses we identified during our fiscal year 2000 audit place FMS's financial systems at significant risk of fraud, unauthorized disclosure and modification of sensitive data and programs, misuse or damage to computer resources, or disruption of critical operations. In addition to the new weaknesses, we found that FMS still needed to act on approximately 42 percent of the weaknesses discussed in our fiscal year 1999 report.[2] 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.

We also assessed the general and application computer controls over key FMS financial systems that the FRBs maintain and operate and have

[1] 31 U.S.C. 331(e) (1994).

[2] *Financial Management Service: Significant Weaknesses in Computer Controls* (GAO/AIMD-00-305, Sept. 26, 2000).

issued a separate letter to the Board of Governors of the Federal Reserve System.[3]

Results in Brief

FMS's overall security control environment continues to be ineffective in identifying, deterring, and responding to computer control weaknesses promptly. Consequently, billions of dollars of payments and collections are at significant risk of loss or fraud, sensitive data are at risk of inappropriate disclosure, and critical computer-based operations are vulnerable to serious disruptions. Based on the results of our fiscal year 2000 audit, we continue to consider FMS's computer control problems a material weakness.[4] FMS officials have also recognized the serious nature of these problems. They have reported these matters as a material weakness to Treasury for fiscal years 2000, 1999, and 1998 following the annual evaluation of internal accounting and administrative controls required to be performed by 31 U.S.C. 3512 (d), commonly referred to as the Federal Managers' Financial Integrity Act (FMFIA). Treasury has also recognized the nature of this problem and reported FMS's computer control problems as a material weakness in *The Secretary's Letter of Assurance* included in Treasury's annual accountability reports for each of those fiscal years.

During our fiscal year 2000 audit, we found new general computer control weaknesses in the entity-wide security management program, access controls, and system software. We also identified new weaknesses in the authorization and completeness controls over one key FMS financial application. Our follow-up on the status of FMS's corrective actions to address weaknesses discussed in our fiscal year 1999 report found that as of September 30, 2000, FMS had corrected or mitigated the risks associated with 35 of the 61 computer control weaknesses discussed in that report. To assist FMS management in addressing its computer control weaknesses, we made four overall recommendations. One of these recommendations refers to 85 detailed recommendations included in the Limited Official Use version of this report.

[3] *Federal Reserve Banks: Areas for Improvement in Computer Controls* (GAO-02-266R, Dec. 10, 2001).

[4] 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.

In commenting on a draft of this report and our more detailed Limited Official Use report, FMS stated that it understands that additional improvements are needed and recognizes the importance of having an effective entity-wide security program, as well as strong internal control, given its critical payment, collections, and government-wide accounting responsibilities. FMS also stated that actions were underway to address the individual audit findings. Further, FMS stated that computer security remains one of FMS's top priorities and that it is completely dedicated to fully implementing and maintaining an effective and robust security program.

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 2000, the U.S. government disbursed over $1.9 trillion primarily for Social Security and veterans' benefit payments, Internal Revenue Service (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 2000, the government collected over $2 trillion in taxes, duties, and fines. 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 multiple financial and information systems to help it process and reconcile moneys disbursed and collected by the various government agencies. These banking, collection, and disbursement systems are also used to process agency transactions, record relevant data, transfer funds to and from the Treasury, and facilitate the reconciliation of those transactions. FMS has three data centers and also has three field operations centers that are responsible for issuing paper check and electronic funds transfer payments. In addition, FMS relies on a network of four contractor data centers and the FRBs to help 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's key financial management systems and to determine the status of the computer control weaknesses discussed in our fiscal year 1999 audit report. 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 financial 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).[5] 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 2000 review at each of the selected data centers and for the key financial applications.

During the course of our work, we communicated our findings to FMS management, which informed us of the actions FMS planned or had taken to address the weaknesses we identified.

We performed our work from August 2000 through February 2001 in accordance with U.S. generally accepted government auditing standards. We requested comments on a draft of this report from the Department of the Treasury. The comments are discussed in the "Agency Comments and Our Evaluation" section of this report and reprinted in appendix II.

FMS's Entity-Wide Security Management Program Continues to Be Ineffective

An entity-wide program for security 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 entity-wide security management program helps to ensure that security controls are adequate, properly implemented, and applied consistently across the entity and that responsibilities for security are clearly understood.

The overriding reason that computer control problems at FMS continued to exist during fiscal year 2000 is that FMS does not have an effective entity-wide computer security management program (security program). In response to our prior years' recommendation that FMS establish an effective security program, FMS completed its *Information Technology*

[5] GAO/AIMD-12.19.6, Jan. 1999.

Security Handbook for Major Application Systems in late 1999. During fiscal year 2000, the *FMS Information Technology Security Policy Manual* and *Entity-Wide Information Technology Security Program* manuals were approved and distributed. In addition, FMS developed an *Entity-Wide Information Technology Security Program Implementation Strategy* in March 2001. This document discusses FMS's high-level strategy for the full implementation of its security program by a target date of September 30, 2002.

In April 2001, FMS completed an internal assessment to determine the effectiveness of its security program and its initiatives. The assessment was performed using the *Federal Information Technology Security Assessment Framework*[6] (Framework). The Framework provides a method for agency officials (1) to determine the current status of their security programs relative to existing policy and (2) where necessary, establish a target for improvement. The Framework identifies five levels of security program effectiveness—Level 1, Documented Policy; Level 2, Documented Procedures; Level 3, Implemented Procedures and Controls; Level 4, Tested and Reviewed Procedures and Controls; and Level 5, Fully Integrated Procedures and Controls. The five levels measure specific management, operational, and technical control objectives. Each of the five levels contains criteria to determine whether the level is adequately implemented, with each successive level representing a more complete and effective security program. FMS's assessment did not contain an overall determination of the level of effectiveness of its security program. Our review of its assessment found that FMS identified as not being met 29 of the 45 control objectives that should be applied to a secure system and another 15 control objectives in which some aspects of the related performance criteria were identified as being partially met.

As discussed above, FMS has taken steps toward improving its security program by developing policy manuals, an implementation strategy, and an internal self-assessment. Through its self-assessment, FMS has identified areas within its existing security program that need improvement in order to achieve a fully implemented Level 5 security program. However, FMS has not yet developed a detailed plan that

[6]*Federal Information Technology Security Assessment Framework*, prepared by the National Institute of Standards and Technology (NIST), Computer Security Division, Systems and Network Security Group, November 28, 2000. Incorporated as Appendix C of NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, August 2001.

describes the remedial actions; resources (physical, human capital, and fiscal); target dates; and responsible agency officials needed to correct the shortcomings of its security program. A Level 5 security program is described as a comprehensive and integral part of an agency's organizational culture. The components of a fully integrated Level 5 security program include

- an active entity-wide security program that achieves cost-effective security,
- integration of information technology security through all aspects of the information technology life-cycle,
- understanding and management of security vulnerabilities,
- continual evaluation of threats and adjustment of controls to the changing security environment,
- identification of additional or more cost-effective security alternatives as the need arises,
- measurement of the costs and benefits of security, and
- establishment of status metrics to assess the effectiveness of the security program that are also met.

FMS's entity-wide security control structure has yet to address many of the weaknesses and related significant risks associated with its current and evolving computing environment. Our audits for fiscal years 2000, 1999, 1998, and 1997 have identified significant general computer control weaknesses at each of the FMS data centers. As shown in table 1, these weaknesses have involved each of the six general control areas defined in FISCAM at multiple FMS data centers.

Table 1: Areas Where Significant General Control Weaknesses Were Identified at FMS Data Centers

Data center	Entity-wide security management program	Access controls	System software	Application software development and change controls	Segregation of duties	Service continuity
			Fiscal year 1997			
1	X	X	X	X	X	X
2	X	X			X	X
3		X		X	X	X
4		X	X	X		
5		X		X		X
6	X	X	X	X		X
7	X	X		X		X
			Fiscal year 1998			
1	X	X	X	X	X	X
2	X	X			X	X
3		X		X		X
4		X	X	X		
5		X		X		
6	X	X	X	X		X
7	X	X	X	X		X
			Fiscal year 1999			
1	X	X	X	X	X	X
2		X		X		
3		X			X	
4		X				
5		X				
6	X	X	X	X		
7	X	X				
			Fiscal year 2000			
1	X	X	X		X	X
4	X	X	X			
5		X				
6	X	X	X	X		
7		X	X			

Source: GAO's analysis of current and prior years' audits results.

If FMS had a fully developed, implemented, and effective security program, weaknesses found in prior years, such as the following, would be less likely to reoccur. For example, at one data center, we found access control weaknesses during our fiscal year 2000 audit that were the same as or very similar to issues that we reported at other data centers in previous years' audits. Although FMS took corrective actions to address the individual prior years' weaknesses found at those specific data centers,

FMS did not determine whether these weaknesses also existed at their other data centers that were using the same type of computing platform. Another example involved a data center that performed security violation and sensitive activity monitoring procedures over its legacy environments. However, FMS did not apply these same procedures and requirements to a new computing environment introduced during fiscal year 2000. Until FMS takes a more disciplined and structured approach to computer security through a fully implemented entity-wide security program, there is a significant increased risk that controls will not be adequate, properly implemented, or applied consistently across each of its data centers.

Integral to all security programs is a continuous risk assessment process for determining the sensitivity of information and systems, acceptable levels of risk, and specific controls needed to provide adequate security over computer resources and data. Our May 1998 best practices guide[7] 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. During our fiscal year 2000 audit, we found that FMS had not developed a comprehensive entity-wide risk assessment to be used as a basis for establishing appropriate security policies and selecting cost-effective techniques for implementing policies. Documents and approaches that FMS had already developed could be used together to form the foundation of an entity-wide risk assessment. The absence of a comprehensive risk assessment that identifies entity-wide risks could lend itself to practices that are inconsistent with acceptable standards and expose FMS to increased weaknesses and unnecessary risks.

Serious General Computer Control Weaknesses Place FMS's 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. In addition to an entity-wide security management program discussed above, they include 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) protect data, files, and programs from unauthorized access, modification, and destruction; (2) limit and monitor access to programs

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

and files that control computer hardware and secure applications; (3) prevent the introduction of unauthorized changes to systems and applications software; (4) prevent any one individual from controlling key aspects of computer-related operations; and (5) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

In addition to the weaknesses in its security program discussed above, our fiscal year 2000 review of FMS's general computer controls also identified serious new general control weaknesses in access controls and system software.

As we previously reported for fiscal years 1998 and 1999, FMS is continuing the process of moving one of its key financial applications to a distributed environment. As of June 30, 2001, FMS reported that approximately 81 percent of the users had converted to a new version of this application, and completion of the new application's implementation was scheduled for September 30, 2001.[8] FMS officials have informed us that they expect that the migration of its key financial application will facilitate the implementation of more effective controls in the future.

Our fiscal year 2000 audit found that as of September 30, 2000, FMS had corrected or mitigated the risks associated with 35 of the 61 computer control weaknesses discussed in our prior year's report. However, we are continuing to reaffirm our prior year's recommendations to correct the remaining weaknesses discussed in our fiscal year 1999 report because of the significance of the associated risks and the lack of other effective compensating controls to mitigate those risks.

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

[8]In commenting on the Limited Official Use version of this report, FMS stated that for this system all of the subapplications except one were implemented, and the remaining one is scheduled for implementation in December 2001.

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 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's access controls identified a number of weaknesses at all of the sites we visited. These weaknesses, many of which were included in our prior years' reports, included data centers that

- had weak network security configurations that allowed us to identify user names and compromise the associated passwords, which resulted in our gaining unauthorized access to the mainframe production environment of a key financial application at one data center, the development environments at another data center, and an unrelated procurement application at a third data center;
- granted excessive and powerful systems privileges to certain users who did not need such access;
- did not effectively manage the administration of certain passwords and user IDs;
- were not always applying security system parameters so as to provide optimum security or appropriate segregation of duties; and
- were not effectively monitoring and controlling dial-in access to certain local area networks and the mainframe environments.

In addition, physical security controls at three of the five sites we visited were not sufficient to control physical access to these centers. For example, at one data center management was not able to provide us with a list of individuals granted physical access to the building because the security system was not functioning properly.

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 many of the sites visited. Because of these identified access control weaknesses, 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.

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.

During our fiscal year 2000 audit, we found system software weaknesses at four of the five sites we visited. Specifically, we found duplicate software modules in certain libraries, lack of procedures to ensure system software changes were properly documented, and the inability for a system to generate reports needed to monitor user activities. These weaknesses increase the risk of obsolete or inappropriate versions of a program executing and causing unexpected results, unauthorized changes to system software, or unauthorized access to sensitive systems.

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 weakness at one of the five FMS sites we visited. As we reported in the prior year, we found during our fiscal year 2000 audit that a significant weakness at the site was that policies and procedures over system design, development, and modification were not established, were inadequate, or were simply not being followed. Without other effective compensating controls in place, failure to implement a disciplined approach to application software development and change controls may result in changes that are not tested, documented, or approved.

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

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.

As we reported in the prior year, we also found during our fiscal year 2000 audit that the programmers at one data center were also serving as backup computer operators, which significantly increases the risk for unauthorized or inappropriate changes to production data and source code or disclosure of sensitive data.

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 ranked 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.

During our fiscal year 2000 follow-up review of FMS's service continuity, we found that FMS management was still in the process of developing an entity-wide service continuity plan. Consequently, the FMS data centers were still at significant risk that in the event of an emergency or disaster, data center personnel might not be prepared to effectively prioritize recovery activities, integrate recovery steps, 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 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 2000 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, protect system software from unauthorized access, and ensure continued computer operations.

FMS's Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs, which are used to perform certain types of work, such as generating 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

Authorization controls for specific applications, similar to general access controls, should be established to (1) ensure individual accountability and proper segregation of duties, (2) ensure that 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 fiscal year 2000 review of FMS's authorization controls found that a number of the weaknesses discussed in our fiscal years 1998 and 1999

reports remained uncorrected and certain new weaknesses over one key financial application were identified. These weaknesses included

- 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,
- users sharing IDs or being assigned multiple IDs without a functional requirement,
- security reports not being consistently monitored or followed up on,
- application passwords not being properly managed,
- lack of certain user access request documentation and recertifications, and
- lack of documented policies and procedures for an application.

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 disruption of operations.

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 fiscal year 2000 review of completeness controls over one key FMS financial application found that input data edit and validation procedures were not complete, software needed to monitor modifications to the database was not in place, and application recovery policies and procedures were not written. As a result, there was an increased risk of processing incomplete or erroneous data and disruption of operations.

FRB Computer Controls Can Be Improved

Because the FRBs are integral to the operations of FMS, we assessed the effectiveness of general and application controls that support key FMS financial systems maintained and operated by the FRBs. Overall, we found that the FRBs had implemented effective general and application controls. Our fiscal year 2000 audit procedures identified certain new vulnerabilities in general controls that did not pose significant risks to the FMS financial systems but nonetheless warranted FRB management's attention and action. These included vulnerabilities in general controls over (1) access to data, programs, and computing resources; (2) system software; and

(3) service continuity. Our follow-up work found that the FRBs had corrected or mitigated the risks associated with all of the vulnerabilities that were identified in our prior year's report. We provided details of these matters in a separate letter 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 related to FMS systems that we identified.

Conclusion

The pervasiveness of the computer control weaknesses—both old and new—at FMS and its contractor data centers place billions of dollars of payments and collections at risk of loss or fraud. Sensitive data are at risk of inappropriate disclosure, and computer-based operations are at risk of disruption. The severity of these risks magnifies as FMS expands its networked environment through the migration of its financial applications from mainframes to client-server 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's operations and computer resources are to be properly protected. It will take a significant and sustained commitment by FMS's management to fully address its serious computer control weaknesses, including fully implementing an effective security program.

Recommendations

In our December 14, 2001, Limited Official Use version of this report, we reaffirmed our prior year's recommendations that the secretary of the Treasury direct the commissioner of the Financial Management Service, along with the assistant commissioner for information resources,

- to fully implement an effective security program,
- to correct each individual weakness that we identified and address each of the 85 specific recommendations detailed in the December 14, 2001 report, and
- to work with the FRBs to monitor corrective actions taken to resolve the computer control vulnerabilities related to FMS systems supported by the FRBs that we identified and communicated to the FRBs.

In addition, we recommended that FMS develop a detailed plan that describes the remedial actions, resources, target dates, and responsible agency officials to facilitate the implementation of its security program.

Agency Comments and Our Evaluation

In commenting on a draft of the Limited Official Use version of this report, FMS stated that it understands that additional improvements are needed and recognizes the importance of having an effective entity-wide security program, as well as strong internal control, given its critical payment, collections, and government-wide accounting responsibilities. FMS also stated that actions were under way to address the individual audit findings. Further, FMS stated that computer security remains one of FMS's top priorities and that it is completely dedicated to fully implementing and maintaining an effective and robust security program.

FMS also stated that it has made great strides in eliminating the vulnerabilities caused by old legacy systems and obsolete technology, resulting in a significant reduction in risks that is not reflected in our report. We believe the report adequately reflects such progress for actions taken by FMS during fiscal year 2001. In particular, our report noted that continued progress has been made in the replacement of FMS's key financial application (which is used by federal agencies to account for their disbursement and receipt activities) by a new version of the application on a distributed computing platform. However, our work over the past 4 years has continued to identify serious issues at FMS. As we stated in our report, FMS's entity-wide security control structure has yet to address many of the weaknesses and related significant risks associated with its current and evolving computing environment. For example, we found that FMS's corrective actions were not being implemented on an entity-wide basis. Weaknesses found and corrected in prior years at certain data centers were identified during the current year audit at another data center. These weaknesses in FMS's computer security controls not only affect the effectiveness of computer security over the new applications recently moved to distributed environments, but also FMS's other key financial applications that are used to collect from and pay to the public billions of dollars annually.

In its comment letter, FMS pointed out that the general consensus of the members of the Treasury CIO Council is that a computer security program that achieves Level 3 effectiveness (which is reached when computer security procedures and technical controls are implemented) is an appropriate standard and should be the department's objective. However, we believe that an effective entity-wide security program is achieved at Level 5 and is the appropriate level for Treasury given its government-wide responsibilities as financial manager, central disburser, and collections agency as well as accountant and reporter of financial information. The need for Treasury to implement an effective and fully integrated entity-wide security program is further underscored by recent events and reports

that critical federal operations and assets continue to be highly vulnerable to computer-based attacks. It is important to note that until an entity has accomplished the Level 4 goal that requires the testing of security procedures and technical controls, it does not have reasonable assurance that the documented controls developed in Levels 1 through 3 have been effectively implemented. A fully integrated Level 5 security program helps to ensure that an organization has incorporated the fundamental activities needed to manage information security risks cost-effectively and is not reacting to individual problems on an adhoc basis only after a problem has been detected. Since FMS's systems process and account for billions of dollars in transactions, we are encouraged that FMS has a goal of continuing to strive for a high level of security effectiveness. While its near term goal of achieving Level 3 effectiveness is commendable, we cannot overemphasize the need for FMS management to make a focused and sustained commitment to accelerate the full implementation of an effective entity-wide security program.

We will follow up on these matters during our audit of the federal government's fiscal year 2001 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 the chairmen and ranking minority members of the Senate Committee on Appropriations; Senate Committee on Finance; Senate Committee on Governmental Affairs; Senate Committee on the Budget; Subcommittee on Treasury and General Government, Senate Committee on Appropriations; House Committee on Appropriations; House Committee on Ways and Means; House Committee on Government Reform; House Committee on the Budget; Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, House Committee on Government Reform; and Subcommittee on Treasury, Postal Service, and General Government, House Committee on Appropriations. We are also sending copies of this report to the commissioner of the Financial Management Service, the inspector general of the Department of the Treasury, the director of the Office of Management and Budget, and other agency officials. Copies will also 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, Daniel G. Mesler, and Mickie E. Gray.

Sincerely yours,

Gary T. Engel
Director
Financial Management and Assurance

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 financial application is subjected to a full-scope review that includes testing in all of the computer control areas defined in the 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 2000 included follow-up on weaknesses discussed in our fiscal year 1999 report and

- a focused review at three data centers of the two general control areas intended to
  - protect data, files, and programs from unauthorized access, modification, and destruction and
  - limit and monitor access to system software programs and files that control computer hardware and secure applications;
- a focused review at a fourth data center of the three general control areas intended to
  - protect data, files, and programs from unauthorized access, modification, and destruction;
  - prevent the introduction of unauthorized changes to systems and applications software; and
  - ensure the recovery of computer processing operation in case of a disaster or other unexpected interruption.

We limited our work at another data center to a follow-up review of the status of weaknesses discussed in our fiscal year 1999 report.

We limited our testing of FMS's entity-wide security program to a comparison of FMS's information security manuals with our executive guide on information security management.[1]

We performed a full-scope application control review of one key FMS financial application to determine whether the application is designed to ensure that

[1] *Executive Guide: Information Security Management* (GAO/AIMD-98-68, May 1998).

- 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 format, and entered into the application accurately, completely, and promptly;
- 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.

We limited our work over another seven key financial applications to a follow-up review of the status of weaknesses discussed in our fiscal year 1999 report.

To evaluate the general and application controls, we identified and reviewed FMS's information system general and application control policies and procedures; observed controls in operation; conducted tests of controls, which included selecting items using a method in which the results are not projectable to the population; and held discussions with officials at selected FMS data centers to determine whether controls were in place, adequately designed, and operating effectively. We performed network vulnerability assessment testing at three data centers. Through our network security vulnerability assessments, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of appropriate FMS officials. The scope of our network vulnerability assessment testing was limited by a fourth data center to a review of a redacted report prepared by other auditors.

Because the FRBs are integral to the operations of FMS, we followed up on the status of the FRBs' corrective actions to address vulnerabilities discussed in our fiscal year 1999 report. We assessed general controls over FMS systems that the FRBs maintain and operate, and we evaluated application controls over two key FMS financial applications.

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. We performed our work from August 2000 through February 2001 in accordance with U.S. generally accepted government auditing standards.

Appendix II: Comments from the Department of the Treasury

COMMISSIONER

DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
WASHINGTON, D.C. 20227

November 9, 2001

Mr. Jeffrey C. Steinhoff
Assistant Comptroller General
United States General Accounting Office
Washington, DC 20548

Dear Mr. Steinhoff:

We appreciate the opportunity to comment on the draft General Accounting Office (GAO) Audit Report, *Financial Management Service: Significant Weaknesses in Computer Controls Continue*, dated October 11, 2001. The Financial Management Service (FMS) recognizes the importance of having in place an effective entity-wide security program, as well as strong internal controls, given our critical payments, collections and government-wide accounting responsibilities. While FMS continues to make significant progress in strengthening computer and security controls, I also understand that we need to make additional improvements. I would, however, like to take the opportunity to provide a more accurate picture of our computer security posture than is portrayed in the report due to the fact that it is based on data that is more than one year old.

FMS has made significant progress in implementing a mature and effective entity-wide security program. We are now following a logical and structured approach to address vulnerability and to prevent unnecessary risk and exposure in internal FMS, fiscal and financial agent, and contractor operated systems. This has significantly reduced the vulnerability and exposure of our systems.

In particular, we have made great strides in eliminating the vulnerabilities caused by old legacy systems and obsolete technology. As an example, FMS has made steady progress in replacing the old Government On-Line Accounting Link System (GOALS) applications to resolve the weaknesses and risks identified in your reports. All of the eight GOALS applications except the Intragovernmental Payment and Collection System (IPAC) have been successfully implemented on new computing platforms, and IPAC is scheduled for implementation in December 2001. This progress - and the significant reduction in risk as a result of these actions - is not reflected in your report.

We have also made improvements in ensuring that the systems operated by the Federal Reserve Banks (FRB) as our fiscal agent have adequate security and control. This year we obtained and reviewed the Federal Reserve's Information Security Manual, and received a letter of assurance from the Board of Governors, as well as a copy of the letter from the Federal Reserve's independent auditor on the integrity of the FRB's processes, including our systems. Furthermore, we received letters of assurance from the District Banks and the Board indicating that FMS systems operated and maintained by the Banks are in compliance with the standards and requirements set forth in the Federal Reserve's

Information Security Manual. I feel comfortable that the vulnerability of our systems at the Federal Reserve, if any, is within acceptable risk.

As part of a Treasury Chief Information Officer Council effort, we took a leadership role along with our partner, the Internal Revenue Service (IRS), in the development of a performance matrix to conduct assessments of all of the Treasury bureaus' entity-wide security programs. The assessment methodology is based on the National Institute of Standards and Technology (NIST) Federal Information Technology Security Assessment Framework (FITSAF). Although the GAO draft report makes reference to Level 5 of the FITSAF, it is the general consensus of the Treasury CIO Council that Level 3 is an appropriate standard and should be the Department's objective. It is our goal to continue to strive for a high level of maturity in the security area but in a cost-effective and business needs driven manner. Achieving Level 3 maturity is our near-term target.

I am fully aware of the need to address individual audit findings, and we are doing that at the same time we are devoting more resources and emphasis to the full implementation of the entity-wide security program and prevention of new vulnerabilities. This has included:

- Introducing and institutionalizing business process risk assessment to identify internal and technical controls earlier in the development lifecycle. This process has been applied to address both technology and business process related security requirements in the earliest stages of the Secured Payment System initiative and our Internet infrastructure build out project.

- Conducting a threat assessment of the Enterprise platform in FY 2000 and updating the assessment in FY 2001.

- Taking a pro-active role in conducting vulnerability assessments of our IT assets as part of the overall risk management program. For example, we are in the process of completing vulnerability assessments on all of our internal IT facilities (including the Regional Finance Centers) and IT operational personnel, as well as actively conducting first level security reviews of our IRS Lock Box service providers.

- Completing a networked-based security assessment of our development and production mid-tier computing platforms using third generation security analysis tools, and acting on that assessment.

- Conducting annual self-assessments of the entity-wide security program in accordance with FITSAF. This year we will also be conducting a self assessment on all application systems utilizing the methodology set forth in the NIST publication, "Self Assessment Guide for Information Technology Systems."

- Most importantly, we have also made significant progress in the areas of disaster recovery and continuity of operations. We completed the build out of a disaster recovery site in our Kansas City office and successfully tested the recovery of our most critical application systems, Payments. In the event of an emergency, we believe we are prepared to quickly and effectively recover all payment operations and are now in a position to extend that recovery capability to other critical FMS systems.

It is my belief that we have made substantial progress in our computer and security controls and we have a maturing entity-wide security program. As a result, we have reduced the vulnerability and exposure of our systems. Although there is always room for improvement, I believe that we have not compromised the public trust in carrying out our payments, collections and government-wide accounting responsibilities. I can assure you that computer security remains one of FMS' top priorities and we are completely dedicated to fully implementing and maintaining an effective and robust security program.

Sincerely,

Richard L. Gregg

Richard L. Gregg

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily e-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

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

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

Visit GAO's Document Distribution Center

GAO Building
Room 1100, 700 4th Street, NW (corner of 4th and G Streets, NW)
Washington, D.C. 20013

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm,
E-mail: fraudnet@gao.gov, or
1-800-424-5454 or (202) 512-7470 (automated answering system).

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G. Street NW, Room 7149,
Washington, D.C. 20548