Notice:

This document does not currently comply with Section 508 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794d. The OIG is working to become fully compliant with the provisions of Section 508. If you need assistance with accessing the file, please contact the OIG's Office of Audit at (202) 927-5400, or **webmaster@oig.treas.gov** for an accessible edition of the report.

This report has been reviewed for public dissemination by the Office of the Counsel to the Inspector General. Information requiring protection from public dissemination has been redacted from this report in accordance with the Freedom of Information Act, 5 U.S.C. section 552.

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

GOVERNMENT-WIDE FINANCIAL MANAGEMENT SERVICES: FMS Continues To Improve Its Controls Over the Access, Disclosure, and Use of Social Security Numbers By Third Parties

OIG-03-083 **May 20, 2003**

Office of Inspector General

****

The Department of the Treasury

Contents

Audit Report 1

Results in Brief 2

Background 3

Findings and Recommendations 4

FMS Has Strengthened Its Privacy Act Program To Ensure That It Makes Legal and Informed Disclosures of SSNs 4

FMS Needs To Better Document, Maintain, and Monitor Third Party Agreements 6
Recommendations 12

FMS Needs To Strengthen Its General Security Controls Over IT Applications and Systems 15
Recommendations 25

FMS' Responses To GAO's Questionnaire Were, In Some Cases, Incomplete and/or Inconsistent 28

Appendices

Appendix 1: Listing of FMS' Systems Containing SSNs [redacted]
Appendix 2: Objectives, Scope, and Methodology 33
Appendix 3: Management Response 34
Appendix 4: Major Contributors To This Report 40
Appendix 5: Report Distribution 41

Abbreviations

BSC	Benefit Security Card
DCIA	Debt Collection Improvement Act
[redacted]	
FAR	Federal Acquisition Regulation
FMS	Financial Management Service
FPA	Federal Program Agency

Contents

FRB	Federal Reserve Bank
FRS	Board of Governors of the Federal Reserve System
FY	Fiscal Year
GAO	General Accounting Office
GSA	General Services Administration
IRS	Internal Revenue Service
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCIE	President's Council on Integrity and Efficiency
PMAC	Private Collection Agency Monitoring and Control
SP	Special Publication
SSA	Social Security Administration
SSN	Social Security Number
TFM	Treasury Financial Manual

May 20, 2003

Richard L. Gregg
Commissioner
Financial Management Service

This report presents the results of the Office of Inspector General's (OIG) audit to assess the Financial Management Service's (FMS) controls over the access, disclosure, and use of Social Security Number (SSN) information by third parties. This review was conducted at the request of the President's Council on Integrity and Efficiency (PCIE) in response to a Congressional request regarding Federal agencies' controls over the use of SSNs.

The overall objective of this review was to assess FMS' controls over the access, disclosure, and use of SSN information by third parties. FMS identified 27 automated information systems that contained SSNs (see *Appendix 1*). The generic term "system" is used in this report to mean either a major application or a general support system. The 27 automated information systems that contained SSNs included systems in five of eight FMS' Assistant Commissioner areas. FMS discloses SSNs to Federal agencies, State and local tax agencies, collection agencies, credit bureaus, contractors, Federal Reserve Banks, and financial institutions. FMS disburses more than $1.2 trillion annually representing nearly 950 million Federal payments. These payments include Social Security, veterans' benefits, and income tax refunds to more than 100 million people. Also, FMS collects more than $2 trillion in Federal revenues, oversees a daily cash flow of $10 billion, provides centralized debt collection services to most Federal agencies, and provides government-wide accounting and reporting. FMS uses an individual's SSN as the primary identification number for payment and receipt of revenue. The continued use of SSNs as identifiers is

critical for FMS in its ability to track payments, collect debts, serve customers, and deter fraud.

We conducted our audit work from February 2002 through December 2002 at FMS Headquarters in Washington, D.C., and at its Hyattsville, Maryland location. A more detailed description of our objectives, scope, and methodology is provided as *Appendix 2.*

Results in Brief

We found that FMS has strengthened its Privacy Act Program to ensure that it makes legal and informed disclosures of SSNs to third parties. However, although FMS is taking steps to safeguard SSNs, opportunities exist to improve controls to ensure sensitive information is better protected. We found that FMS needs to better document, maintain, and monitor third party agreements to ensure that security requirements are met.

FMS also needs to strengthen its general security controls over Information Technology (IT) applications and systems. As part of these security controls, FMS needs to complete or improve its: (1) implementation of IT security policies, standards, and procedures; (2) risk analysis process; (3) security planning process; (4) security incident reporting; (5) monitoring of employees' access to computerized records; and (6) IT application and system training.

We also found that FMS' consolidated questionnaire did not always reflect the responses made by the subordinate business areas and that some of FMS' responses to the General Accounting Office (GAO) questionnaire were incomplete and/or inconsistent with what our review determined.

We made 10 recommendations to improve FMS' controls over the access, disclosure, and use of SSNs by third parties.

FMS concurred with our 10 recommendations and has taken or plans to take appropriate corrective actions. FMS efforts to address our audit findings have been on-going throughout the duration of this audit. FMS officials reported that they have

completed 4 of the 10 recommendations. FMS is in the process of implementing the remaining 6 recommendations to (1) modify FMS' existing security policies, standards, and procedures; (2) ensure that FMS' agreements with credit bureaus are updated as required by FMS guidance; (3) ensure that all FMS business areas, fiscal agents, financial agents, and contractors adhere to its revised IT policies, standards, and procedures; (4) continue to improve its security planning process; (5) fully execute the new computer security incident reporting guidelines and capability; and (6) re-certify system users on an annual basis. FMS plans to develop a detailed corrective action plan that will consider all areas of FMS and include realistic timeframes for completing proposed actions. FMS' management response is included in its entirety in *Appendix 3*.

Background

The Social Security Administration (SSA) created the SSN in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. However, over the years, the SSN has become a "de facto" national identifier used by Federal agencies, State and local governments, and private organizations. Government agencies frequently ask individuals for their SSNs because in certain instances they are required to or because SSNs provide a convenient means to track and exchange information. While a number of laws and regulations require the use of SSNs for various Federal programs, they generally also impose limitations on how these SSNs may be used.

Although no single Federal law regulates overall use and disclosure of SSNs by Federal agencies, the Freedom of Information Act of 1966, the Privacy Act of 1974, and the Social Security Act Amendments of 1990 generally govern disclosure and use of SSNs. In addition, a number of Federal laws lay out a framework for Federal agencies to follow when establishing information security programs that protect sensitive personal information, such as SSNs. Most recently, the Government Information Security Reform provisions of the Fiscal Year (FY) 2001 National Defense

Authorization Act require that Federal agencies take specific measures to safeguard computer systems that may contain SSNs.

Due to concerns related to perceived widespread sharing of personal information and occurrence of identity theft, Congress asked GAO to study how and to what extent Federal, State, and local government agencies use and safeguard SSNs. As part of the study, GAO sent questionnaires to 18 Federal agencies that it thought were likely to routinely obtain, maintain, and use SSNs.

While no one can fully prevent SSN misuse, Federal agencies have responsibility to limit the risk of unauthorized disclosure of SSN information. To that end, the Chairman of the House Ways and Means Subcommittee on Social Security asked the SSA OIG and the PCIE to look at the way Federal agencies disseminate and control SSN information.

Findings and Recommendations

Finding 1 FMS Has Strengthened Its Privacy Act Program To Ensure That It Makes Legal and Informed Disclosures of SSNs

We found that FMS has strengthened its Privacy Act Program in numerous ways to ensure that it makes legal and informed disclosures of SSNs to third parties. For example:

- FMS issued to all employees in June 2002, a Privacy Act Overview, a 13-page document to ensure that all employees be aware of and comply with the requirements of the Privacy Act. This document includes information on use and disclosure of SSNs, accounting for disclosures, requests for notification and access, disclosing SSNs to third parties, contractor training, and rules of conduct and penalties for non-compliance.
- The Commissioner, through an e-mail and memorandum to all FMS employees in June 2002, emphasized the importance of protecting individuals' privacy.

- FMS finalized a Privacy Act Policy in September 2002 that (1) established a program to ensure that all FMS employees were aware of and followed the requirements of the Privacy Act relating to the collection, maintenance, use, and dissemination of personal information, including SSNs; and (2) required contracts and financial agency agreements to contain provisions covering third parties' responsibilities regarding the protection of sensitive information and the requirement to train their employees and subcontractors to safeguard the sensitive information.
- Each Assistant Commissioner appointed a Privacy Act liaison officer to monitor FMS' compliance with the Privacy Act and to assist in the implementation of Privacy Act policies.

FMS provides identifying information, including SSNs, to credit reporting agencies as authorized under the Debt Collection Improvement Act (DCIA). The DCIA requires Federal agencies to report information to credit reporting bureaus on all delinquent consumer debts owed to the Federal Government. The credit bureaus must abide by the Fair Credit Reporting Act, which governs maintenance and disclosure of information by credit bureaus.

FMS also provides information, including individuals' SSNs, to contractors including private collection agencies and companies performing research, data gathering or analysis. Government contracts are regulated by the Federal Acquisition Regulation (FAR) and Treasury Department requirements. The FAR requires Privacy Act Notification and Privacy Act clauses in each applicable contract. The Privacy Act clauses require the contractor to comply with the Privacy Act requirements and agency rules and regulations issued under the Privacy Act. The required clauses express penalties for violating the Privacy Act.

FMS informs individuals that their SSNs might be provided to other individuals or organizations by announcement in the Federal Register and/or by written notification on the program application or other forms. The announcement in the Federal Register identifies the records containing SSNs that may be disclosed to appropriate Federal, State, and local agencies and other third

parties for tax collection, payment verification, debt collection or other investigative and enforcement activities. The written notification on the program applications involve those specific applications or forms that an individual is required to complete to receive a benefit from an agency program. For example, individuals participating in an agency program are required to provide their SSN to help ensure proper payment to the correct account.

Individuals who access FMS systems are required to provide their SSN on a registration form, an access request form, and a Dial-in User Agreement. These forms state that all or part of the information may be furnished to Federal, State, local, and public agencies in the event a violation of law is disclosed, and that disclosure of the SSN is mandatory under Executive Order 9397 for use solely as an identifier. Individuals may authorize FMS, its agents, and contractors to make disclosures to other parties by executing the FMS form - Authorization for Release of Information.

Finding 2 FMS Needs To Better Document, Maintain, and Monitor Third Party Agreements

We found that FMS needs to better document, maintain, and monitor third party agreements. FMS did not: (1) have adequate written policies and procedures for establishing and administering programs with its financial agents; (2) have consistent safeguards and Privacy Act clauses in third party agreements and contracts with all its financial agents and contractors, including private collection agencies; (3) provide signed Memorandums of Understanding (MOUs) with the credit bureaus as required; and (4) adequately monitor all FMS systems operated or supported by the financial agents or contractors. As a result, FMS had difficulty identifying all third party employees who had access to or used information from its automated systems and ensuring that all users were valid.

FMS also discloses SSN information to Federal Reserve Banks (FRBs), which act as FMS' fiscal agents. FMS does not use formal MOUs to designate FRBs as fiscal agents or to direct their activities, because FMS believes such agreements are unnecessary

given the congruent working relationship between the agencies. FMS relies on FRB measures and procedures to protect SSN information.

Written Policies and Procedures

At the start of our review, we found that FMS did not have adequate written policies and procedures for establishing and administering programs with its financial agents and contractors. FMS did not require its financial agents to provide identifying information on all employees and applicable contractors working under the various programs. Therefore, FMS could not maintain listings of such employees. As a result, FMS had difficulty identifying all third party employees who had access to or used information from its automated systems and ensuring that all users were valid.

Consistent Safeguards and Privacy Act Clauses

We found that FMS did not have consistent safeguards and Privacy Act clauses in third party agreements and contracts with all its financial agents and contractors, including private collection agencies. This occurred because FMS had not finalized its procedures to ensure appropriate consistency within agreements with its financial agents and FMS applicable contracts and task orders.

The FAR requires Privacy Act clauses in solicitations, contracts, and subcontracts when the design, development, or operation of a system of records on individuals is required to accomplish a specific FMS function. We found that all contracts and task orders involving the systems in our review did not always include the required FAR Privacy Act clauses. Consistency is needed to ensure that responsibilities are established regarding the use of personal information obtained from FMS and to ensure that the wording of each contract makes the provisions of the Act binding on the contractors and the contractor's employees.

We also found that, in two of the agreements with financial agents that FMS provided to us, FMS did not require timely notices of

security incidents involving unauthorized disclosure of personal information.

FMS has taken steps to improve procedures and consistency of Privacy Act clauses. FMS' Privacy Act Policy, issued in September 2002, now requires that all FMS contracts and financial agency agreements include provisions, where applicable, outlining the contractor's and financial institution's responsibilities regarding the use of personal information obtained from FMS. Also, in September 2002, FMS' Assistant Commissioner for Federal Finance developed and issued a policy requiring legal review of financial agency agreements and related documents. In addition, during October 2002, the Office of Chief Counsel was in the process of developing even more explicit provisions on Privacy Act compliance and contractor training requirements for financial agency agreements and related documents. FMS reported that it has task orders with its private collection agencies based on a master contract with the General Services Administration (GSA). FMS believes that the master GSA contract contains appropriate Privacy Act clauses. In our opinion, the Privacy Act clauses in the master contract with GSA would not preclude including the clauses in the applicable subcontracts or task orders with other contractors. FMS is in the process of finalizing the FMS Privacy Act clauses and provisions for agreements with the financial agents and applicable contracts and task orders.

Memorandums of Understanding With Credit Bureaus

FMS did not have signed MOUs with credit bureaus. FMS' *Guide to the Federal Credit Bureau Program* requires a MOU between FMS, as the Federal agency, and the credit reporting bureau. Without such signed MOUs, FMS had not effectively documented responsibilities to the credit bureaus.

FMS provides identifying information, including SSNs, to credit reporting agencies as authorized under the DCIA. The DCIA requires Federal agencies to report information to credit bureaus on all delinquent consumer debts owed to the Federal Government.

In October 2002, we suggested that FMS update its agreements with credit bureaus to conform to FMS' Guidelines. FMS officials agreed with this corrective action and reported that almost all agreements with the credit bureaus have been completed and they are working on finishing the remaining agreements.

Monitoring Third Party Agreements

We found that, at the start of our review, FMS was not adequately monitoring all FMS systems operated or supported by the financial agents or contractors. FMS did not always conduct on-site inspections and/or independent security reviews for all its systems containing SSNs that the agents or contractors operate or support. In addition, for some of the internal security reviews FMS did conduct, there was not adequate time for testing and validation to ensure that policies and procedures were effectively implemented at the site. FMS officials told us that this occurred because of limited resources and the need to review agreements that were due to expire.

According to Office of Management and Budget (OMB) A-130 Appendix III*, Security of Federal Automated Information Resources*, an independent review or audit of security controls should be performed for each application at least once every 3 years. FMS' policy, which is applicable to financial agents and contractors, requires periodic information technology security reviews be conducted for systems processing sensitive information to ensure that security controls are functioning effectively and are providing adequate levels of protection. The security reviews are to be performed annually or after a major enhancement or change which results in significant modification in the operational environment or security controls. Internal or external organizational groups may conduct the security reviews, however an independent party must conduct the reviews, not the business owner.

FMS has taken steps to improve monitoring of its third party agreements. FMS established a Bank Review Office in early FY 2002. This office focuses on reviews of systems and programs operated by financial agents and their contractors.

In addition, FMS' Assistant Commissioner for Federal Finance issued a policy in September 2002, to ensure that systems operated by financial agents, contractors, and fiscal agents are subject to periodic independent third-party reviews. A critical function of these reviews is to ensure that the agents are adequately protecting Privacy Act information in the automated systems. The information processed by these systems requires protection since improper use or disclosure of the information could adversely affect the ability of FMS to accomplish its mission.

Federal Finance is also developing a comprehensive, automated system for reporting and tracking review findings and corrective actions. Contractor adherence to the Privacy Act will be monitored and assessed as a contractor performance measure.

Federal Reserve Banks

FMS had 10 systems containing SSNs that were operated or supported by FRBs. FMS did not have MOUs, written agreements, or documented guidance with FRBs for 8 of these 10 systems. FMS did not have formal MOUs with FRBs, because FMS believed that such agreements were unnecessary given the congruent working relationship between the agencies. Further, it is FMS' opinion that such agreements would not add value to the nature of the work performed by the FRBs. FMS did, however, have written agreements for 2 of the 10 systems because Internal Revenue Service (IRS) tax information was involved. These agreements included various safeguards to protect sensitive information.

FMS discloses SSN information to FRBs, which act as FMS' fiscal agents. FMS has frequently used the FRBs as fiscal agents in providing services or developing and operating systems that rely on payment services given the Federal Reserve's particular expertise in this area. FMS reported that it works closely and collaboratively with the FRBs to ensure that necessary duties are carried out as required.

The FRBs must adhere to policies of the Federal Reserve, including the Federal Reserve Information Security Manual, the Federal Reserve Information Technology Change Management Procedures,

and the Federal Reserve Information Technology Problem Management Procedures. The FRB's compliance with these policies is subject to review by FRB internal auditors and the GAO.

In addition, the Board of Governors of the Federal Reserve System (FRS) continually assesses FRB measures to protect the security of systems containing confidential information. On an annual basis, the Board of Governors provides written assurance to FMS regarding their compliance with the FRB procedures, as well as follow-up on any GAO audit findings impacting its systems. In November 2002, FMS officials informed us that they requested that the FRS provide, as part of its annual assessment, a report on the results of FRB internal system reviews and the status of any findings at the FRB. The FRB agreed to add the additional information to its annual assurance letter. FMS relies on FRB measures and procedures to protect SSN information.

We found that the FMS security policy and standards issued June 26, 2002, stated that they applied to fiscal agents, as well as financial agents and contractors. However, FMS officials stated that the FRBs are not required to follow FMS security policies because FRBs are not Government entities. It is FMS' assessment that the Federal Reserve's standards in this area more than meet the security goals of FMS. FMS officials reported in November 2002, that FMS' existing security policies, standards, and procedures would be revised to document the correct policy for the FRBs.

In lieu of preparing and modifying written agreements, FMS plans to provide guidance to the FRBs regarding FMS requirements by adding a new chapter to the Treasury Financial Manual (TFM). The new guidance in the TFM will address FMS requirements covering all FRBs that access, disclose, or use SSN information to protect the SSN information. A draft of the proposed changes to the TFM was in process during our audit.

Recommendations

The Commissioner should:

1. Strengthen written policies and/or procedures to:

    a. Establish and administer programs with financial agents to ensure that all third party contractor and financial agent employees who have access or use SSN information in its automated systems are validated; and
    b. Ensure that FMS finalize and implement the FMS Privacy Act clauses and provisions for agreements with the financial agents and that the FAR and FMS Privacy Act clauses are included in all applicable contracts and task orders.

    Management Comments

    FMS concurred with the recommendation and has taken corrective action.

    a. FMS has established the Bank Review Office to provide security oversight support for the Government-wide collections program. On-site security reviews are conducted of financial agents and contractor facilities. A critical function of these reviews is to ensure that financial agents have implemented effective security controls with respect to facilities, personnel, and sensitive information associated with government collection activities to prevent theft, compromise, and unauthorized disclosure.
    b. In addition to using the Privacy Act clauses in the FAR when appropriate, FMS drafted supplemental individual Privacy Act clauses to be used in FMS contracts and agreements, as applicable. FMS has implemented internal procedures to ensure that program staff inform its Acquisition Management Division when a requirement includes Privacy Act concerns so that the Acquisition Management Division can include the appropriate clauses in contracts and task orders.

Privacy Act clauses are also incorporated into financial agreements when appropriate.

OIG Comments

The OIG believes that the actions taken by FMS address the intent of the recommendation.

2. Ensure that FMS' agreements with credit bureaus are updated to conform to the MOU contained in FMS' *Guide to the Federal Credit Bureau Program*.

Management Comments

FMS concurred and stated that it has updated 6 of 7 required agreements with the credit bureaus used in its debt collection program to conform to the MOU contained in FMS' *Guide to the Federal Credit Bureau Program*. According to its April 22, 2003 management response, FMS expects the last agreement to be signed within the next week. If not received as promised, FMS will stop reporting consumer debt to the credit bureau that has failed to sign the necessary MOU.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

3. Continue to monitor the activities of contractors, financial agents, and fiscal agents to ensure that sensitive information is safeguarded as required, including the requirement to conduct periodic independent third party reviews.

Management Comments

FMS concurred and stated that it has established the Bank Review Office to provide security oversight support for the Government-wide collections program, and to ensure that an aggressive, proactive approach is taken to identify and

address security weaknesses and instances of non-compliance with applicable Treasury directives/requirements.

Contractor adherence to the Privacy Act will be monitored and assessed as a contractor performance measure. As a matter of practice, both performance-based service contracts and nonperformance-based service contracts will reflect this as a performance measure and reporting requirement. FMS contractors will be assessed on this element in our past performance database. Debt Management Services and other areas will continue to monitor the activities of contractors to ensure that sensitive information is safeguarded.

Federal Finance has implemented a policy to ensure that systems are subject to periodic independent third-party reviews. In addition, Federal Finance has also developed a comprehensive, automated system for reporting and tracking incidents, review findings, and corrective actions.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

4. Modify security policies and standards dated June 26, 2002, to reflect the new requirements for FRBs as fiscal agents.

Management Comments

FMS concurred and stated that it is in the process of implementing this recommendation to modify FMS' existing security policies, standards, and procedures to reflect the correct requirements for the FRBs.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

5. Ensure that the new chapter of the TFM is revised and implemented as planned.

Management Comments

FMS concurred and stated that the new chapter of the TFM was published on March 4, 2003. The chapter reflects the existing practices of the FRBs with respect to the protection of information.

OIG Comments

The OIG believes that the actions taken by FMS address the intent of the recommendation.

Finding 3 FMS Needs To Strengthen Its General Security Controls Over IT Applications and Systems

We found that FMS needs to strengthen its general security controls over Information Technology (IT) applications and systems to ensure SSN information is better protected. As part of these security controls, FMS needs to complete or improve its: (1) implementation of IT security policies, standards, and procedures; (2) risk analysis process; (3) security planning process; (4) security incident reporting; (5) monitoring of employees' access to computerized records; and (6) IT application and system training. FMS needs to strengthen its general controls to ensure that a structured process is in place to maintain adequate cost-effective security requirements and that its IT program is able to respond to the rapidly changing technological environment.

An OIG audit report, *Audit of the Financial Management Service's Fiscal Years 2002 and 2001 Schedules of Non-Entity Government-Wide Cash,* OIG-03-039, dated December 23, 2002, considered FMS' computer control problems to be a material weakness. In the area of computer controls, there were numerous general controls weaknesses at the [redacted] that did not effectively prevent (1) unauthorized access to and disclosure of

sensitive information, (2) unauthorized changes to systems and applications software, (3) unauthorized access to certain programs and files, or (4) disruption of critical operations. The report also identified weaknesses in certain application controls and disclosed an instance of noncompliance relating to OMB Circulars A-127 and A-130, which require a comprehensive security plan and controls to protect information.

OMB Circular A-127, *Financial Management Systems,* states that each agency shall plan for and incorporate security controls in accordance with the Computer Security Act of 1987 (Computer Security Act). OMB Circular A-130, *Security of Federal Automated Information Resources*, states that agencies are required to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in systems. Adequate security also includes ensuring that the systems used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability. Inadequate security may result in loss, misuse, or unauthorized access to or modification of information.

IT Security Policies, Standards, and Procedures

At the start of our audit, we found that FMS did not initially have IT policies, standards, or procedures that specifically addressed the access, disclosure, and use of [redacted] information. FMS was able to provide us with general IT policies, standards, and procedures. The establishment and implementation of specific policies, standards, and procedures will ensure that FMS has adequate security for the information collected, processed, transmitted, stored, or disseminated in its automated systems. Accordingly, FMS subsequently revised its September 2000 policies and procedures and established better IT standards in June 2002, which our review determined were adequate.

OMB Circular A-130 requires each agency to develop and implement policies, standards, and procedures that are consistent with government-wide policies, standards, and procedures issued by the OMB, the Department of Commerce, GSA, and the Office of Personnel Management (OPM).

IT policies are established principles mandated by Federal laws, regulations, Executive Orders, the Treasury Department, and other executive agencies. IT standards are expansions of the IT policies that outline security controls, safeguards and illustrations of how to consistently apply the established IT policies. IT procedures are activities and tasks developed to execute the IT standards and to assign responsibilities to individuals.

In June 2002, FMS IT officials submitted revised FMS IT policies and procedures with improved IT standards. These revised IT policies, procedures, and standards were part of a recent FMS initiative to enhance its Entity-Wide IT Security Program. The FMS IT policies, standards, and procedures address the requirements for securing, protecting, storing, retaining, and destroying sensitive information and data maintained on FMS' systems. Sensitive information is defined as the data FMS uses to conduct its mission including all personnel/personal data maintained regarding employees and contractors who carry out the FMS mission.

We found the revised IT policies, standards, and procedures to be adequate. However, we found that several aspects outlined in the revised IT policies, standards, procedures were not fully implemented. For example, system risk assessments were not performed; security plans were not completed; the FMS written computer security incident reporting plan was not implemented and account management procedures were not executed for all the systems with SSNs. FMS officials indicated that its Entity-Wide IT Security Program is evolving and a vast amount of progress has been made; however, additional work to the program is still needed.

Risk Analysis Process

Although we found that FMS had an adequate risk management policy in place, FMS did not perform periodic system risk assessments for 24 of its 27 systems. Risk assessments are a means of providing decision makers with factors that can negatively influence operations and potential outcomes. Also, risk assessments provide management with information to make informed judgments concerning the extent of actions needed to

reduce risks. Risk assessments are important to determine if IT security requirements are being satisfied and to ensure that appropriate, cost-effective safeguards are incorporated in all new and existing FMS systems.

OMB Circular A-130 requires agencies to conduct risk assessments on all automated systems. Furthermore, FMS policy requires a risk analysis process to be established and maintained to determine the specific vulnerabilities and threats associated with IT resources throughout the system's lifecycle. FMS' risk management establishes the requirement for risk analyses to use the principle of risk assessments.

Although FMS did not conduct system risk assessments, FMS conducted business risk assessments for various business areas in which systems with SSNs are critical assets. FMS officials informed us that the business risk assessments were not intended to be a replacement for system risk assessments. FMS officials informed us that it is their intention to prepare risk assessment for each system in FY 2003.

Security Planning Process

Although FMS has demonstrated that its security planning process has evolved since the beginning of our audit, we found that FMS needs to ensure that all systems with SSNs have a completed and well-documented security plan. The objective of security planning is to improve protection of IT resources and the ability of these technology resources to protect stored information. The protection of a system must be documented in a security plan. Security plans should provide an overview of the security requirements of the system, describe the controls in place or planned for meeting those requirements, and assign responsibilities and explain expected behavior for all individuals who access the systems.

The completion of system security plans is a requirement of OMB Circular A-130 and Public Law 100-235, Computer Security Act. The Computer Security Act requires that all systems with sensitive information, e.g., SSNs, develop

computer security plans. Furthermore, Federal agencies are required to follow the guidance set forth by the National Institute of Standards and Technology (NIST). NIST Special Publication (SP) 800-18 specifically deals with developing security plans for IT systems.

In April 2002, we requested security plans for all FMS systems that contained SSNs. Initially, FMS could only provide us with 10 system security plans for the 27 systems that contained SSNs. Upon completion of our fieldwork, FMS was able to provide us with 21 security plans for its 27 systems that contained SSNs.

Initially, 7 of the 21 security plans we received were in draft; 10 did not reflect all of the management or operational improvements that were currently being instituted by FMS management; 3 did not meet minimum Federal requirements; and 1 was incomplete. We found that the recently developed FMS Rules of Behavior, information regarding recent security reviews, risk assessments, security incident reporting and authority to operate the systems were not always included in the security plans.

The [redacted] was identified as 1 of the 27 systems that contained SSN information. The FMS Enterprise is composed of five supporting components. When we requested system security plans for the five components of the Enterprise, we received only one security plan for the Mainframe. We consider the Enterprise security plan incomplete due to the absence of the security plans for the other four vital components. IT officials informed us that security plans for the other components of the Enterprise had been contracted to a vendor.

We also found that FMS security plans for two systems -- [redacted] -- did not clearly and completely describe the two systems. FMS officials provided one security plan for the [redacted] and informed us that it incorporated the 26 payment applications located at different Regional Financial Centers. According to the

security plan, each Center has a site-specific physical security plan.

FMS made a decision to consolidate the [redacted] security plan after reviewing Section 2.1, System Boundaries of NIST SP 800-18. Section 2.1 specifies that each element of the system must (1) be under the same direct management control; (2) have the same function or mission objective; (3) have essentially the same operating characteristics and security needs; and (4) reside in the same general operating environment to constitute a single system requiring a security plan. All components of a system need not be physically connected.

Accordingly, FMS is currently certifying the [redacted] as one collective system. However, the single plan provided by FMS did not include specific references to all 26 applications. The plan was very general and discussed payments as one function. The 26 applications were not all separately identified within the security plan. In addition, information about the 26 applications was somewhat different from the information presented in the security plan. The [redacted] is one of FMS' critical systems and the payment function is a very large part of FMS' mission. According to NIST SP 800-18 guidance, the level of detail included within the plan should be consistent with the criticality and value of the system to the organization's mission.

We also found that the [redacted] security plan referred to the [redacted] and the [redacted] as systems and, in some instances, as one system or application. Subsequently, FMS officials reported that [redacted] is not a separate system, but one of the databases included in [redacted]. The critical components of the system should be properly identified throughout the security plan.

FMS was unable to provide us with six security plans. FMS officials informed us that one of the systems, Benefit Security Card, did not have a security plan because it was being eliminated at the beginning of 2003. FMS did not have security plans for five systems maintained or operated by the FRBs.

These five systems were: [redacted]

FMS standards and procedures, revised in June 2002, specifically state that systems operated by the FRBs are required to have system security plans.

Certification and Accreditation

We found only 5 of 27 systems that we reviewed were certified and accredited. Four of the five systems are FRB-operated systems that did not have security plans but were certified and accredited by FMS officials. FMS has authorized another 19 systems with SSNs to operate on an interim basis until the requirements of certification and accreditation can be met. FMS has three remaining systems that are not certified or accredited nor do they have authorization to operate for the interim period.

These three systems are the [redacted], the [redacted], and the [redacted]. FMS officials told us that the [redacted] will be phased out by June 2003, and that a decision has been made not to perform any certifications or accreditations for that system. Recently, FMS officials re-classified the [redacted] and the [redacted] systems as programs and informed us that the two former systems are no longer owned by FMS. Therefore, FMS will not be performing any certifications or accreditations on these programs.

Certification and Accreditation is the process in which a management official must authorize a system to process information or operate based on judgment and understanding of the business needs, security and integrity controls. Treasury and FMS both have established policies, which require security plans be completed prior to certification and accreditation of a system. FMS officials informed us that they are currently working to complete security plans for those systems that are being housed, facilitated and operated by the FRBs. In addition, FMS told us that all of its currently owned systems, that are not

scheduled to be phased out, were placed under Interim Authorization to Operate by August 30, 2002, until the requirements for Certification and Accreditation can be met. FMS plans to complete Certification and Accreditation activities by September 30, 2003.

Security Incident Reporting

Prior to July 2002, FMS did not have a formal written policy for reporting computer security incidents and did not have computer security incident response capability. Failure to develop written policies and to implement computer security incident response capability could impede FMS ability to correctly handle an incident, prevent or minimize disruption of critical computing services, and minimize loss or theft of sensitive or mission critical information.

During our review, FMS provided us with three computer security incidents in which SSN information could have been improperly disclosed and/or potentially misused. Our review of each security incident indicated that FMS had an informal and undocumented reporting process that was effective but may not have been known to all users.

OMB Circular A-130 and Treasury guidelines require agencies to be able to respond to security incidents in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident and to establish formal incident response mechanisms. OMB security guidelines also require all bureaus to establish an incident response capability to ensure that a process exists to help users when a security incident occurs in a system and to share information concerning common vulnerabilities, threats, and corrective actions taken.

In July 2002, FMS issued *FMS Computer Incident Reporting Policy and Response Guide*. This policy provides general guidance to technical and management staff and was designed to enable quick and efficient recovery from security incidents and to carry out all necessary steps to correctly handle an

incident. We found the policy to be adequate and in compliance with OMB Circular A-130. However, FMS officials had not fully implemented its policy by the completion of our fieldwork.

Monitoring Employees Access To Computerized Records

FMS was not effectively and appropriately managing and monitoring users accounts. Prior to July 2002, FMS was not following its policy and standards for the management of user accounts and operating procedures were not developed. Specifically, FMS: (1) did not maintain or track all users access activities in the FMS database repository; (2) was not performing any IT user account re-certification procedures; and (3) did not provide appropriate documentation to determine whether user re-certification processes were being performed for all applications with SSNs. Failure to restrict access to system resources threatens the confidentiality, integrity, and availability of the FMS IT systems and applications.

The FMS [redacted] did not maintain or track all users access activities. FMS policies and procedures indicated that [redacted] was a database repository that would track and monitor all users access information. We found two systems with SSNs that were housed in FMS facilities in which the user access information was not included in [redacted]

Also, FMS was not performing IT user account re-certification procedures. Re-certification is a process used to ensure that all accesses and permissions to FMS IT resources are valid and current. A re-certification process should be performed at both the system and the application levels. The FMS IT staff is responsible for performing the IT user account re-certification process (system level), and the system owners are responsible for conducting a process at each application level.
FMS IT officials developed written procedures for re-certification. However, we were not provided enough documentation to determine whether appropriate monitoring or re-certification procedures were being performed at the application levels. We requested written re-certification

procedures for all 26 applications. We only received procedures for three applications. One of the three procedures was incomplete. Furthermore, although FMS officials for the remaining two applications stated that their process was performed on an annual basis, we were not provided any documentation to support this statement. FMS officials stated that fiscal and financial agents are maintaining documentation of the user accounts and profiles. However, FMS IT staff was not performing any monitoring activities over user access at the fiscal and financial agents locations.

In addition, a prior year audit report, *Management Letter For Fiscal Year 2001 Audit of Schedule of Non-Entity Government-Wide Cash,* OIG-02-077, dated April 15, 2002, found that 8 out of 15 user IDs reviewed lacked documentation for approval to access an FMS system. To resolve the prior year audit finding, FMS IT staff developed an approach that provided system owners with user access information. System owners were requested to validate the information provided. We noted that the information provided to the system owners was limited to FMS employees and contractors only and did not include any of the Federal Program Agency (FPA) users for systems maintained by FMS or systems managed or maintained by contractors, financial agents, or fiscal agents. FMS officials stated that this approach was a "one-time snap-shot" that they were using to create a baseline. FMS completed its IT user re-certification process September 2002, and several changes were made. FMS anticipated starting its annual re-certification process in January 2003.

IT Application and System Training

We found that FMS provided mandatory periodic general IT security education and awareness training. However, many FMS employees, FPAs, and contractors were not provided with training that was specific to the system in which they had access. Specific system training will ensure that employees are knowledgeable in the rules of the systems, federal guidance, available technical assistance, and various technical security products.

The Computer Security Act, OPM, and OMB Circular A-130, all emphasize mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information such as SSNs. FMS management should ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing access to the system.

Recommendations

The Commissioner should:

1. Ensure that all FMS business areas, fiscal agents, financial agents, and contractors adhere to its revised IT policies, standards, and procedures, dated June 2002, and any future revisions.

   Management Comments

   FMS officials concurred and stated that they are taking steps to implement this recommendation. Among other steps, Senior Executives are briefed monthly on IT security issues, concerns, or events. Further, the on-going Certification and Accreditation effort will ensure adherence to IT policies, standards, and procedures. FMS plans to develop a detailed corrective action plan that will consider all areas of FMS and include realistic timeframes for completing proposed actions.

   OIG Comments

   The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

2. Continue to improve its security planning process by ensuring that OMB and NIST guidelines are followed for all systems and major applications by:

   a. Continuing to develop and/or revise the security plans for all systems in accordance with FMS and Federal guidelines.

b. Ensuring that security plans are established prior to the issuance of system certifications and accreditations.
c. Ensuring that system risk assessments are conducted for all systems.

Management Comments

FMS concurred and stated that it is implementing this recommendation for all systems. FMS plans to develop a detailed corrective action plan that will consider all areas of FMS and include realistic timeframes for completing proposed actions.

a. Security plans are being reviewed and/or revised in 2003 as part of the certification process currently underway at FMS. Security plans are currently being developed for all systems running at the FRBs.
b. FMS is updating and/or developing security plans for all operational systems to ensure that such plans are established prior to the issuance of system certifications and accreditations.
c. FMS is completing system risk assessments in 2003 as part of the planned Certification and Accreditation process.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

3. Fully implement the new computer security incident reporting guidelines and institute its computer incident reporting capability as planned.

Management Comments

FMS concurred and stated that it is in the process of implementing this recommendation. FMS plans to develop a detailed corrective action plan that will consider all areas of

FMS and include realistic timeframes for completing proposed actions.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

4. Improve monitoring of user access activities in systems that contain SSNs by:

   a. Implementing re-certification user access procedures within its systems (including fiscal and financial operated systems) as scheduled.
   b. Ensuring that all FMS operated systems are included in the FMS [redacted].

Management Comments

FMS concurred and stated that it plans to develop a detailed corrective action plan that will consider all areas of FMS and include realistic timeframes for completing its proposed actions. FMS is in the process of implementing its recommendation by:

   a. Re-certifying all Enterprise users. The Check Payment & Reconciliation System and the Intra-Governmental Payment and Collection System have re-certified users. The Treasury Offset Program continues to review all users on a quarterly basis. All other applications will be re-certifying users on an annual basis beginning in 2003.
   b. Replacing the [redacted] with the IBM Tivioli Identity Implementation (ITIM) product. The ITIM will include all systems operating on the FMS Enterprise platform.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

5. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing access to the system.

Management Comments

FMS concurred and stated that security training will occur annually. FMS requires that new employee training includes a session on employees' security responsibilities.

OIG Comments

The OIG believes that the actions taken and planned by FMS address the intent of the recommendation.

Finding 4 FMS' Responses To GAO's Questionnaire Were, In Some Cases, Incomplete and/or Inconsistent

FMS submitted a consolidated (entity-wide) response to the GAO questionnaire based on responses from five subordinate questionnaires completed by the five FMS business areas that had applications and/or systems that included SSNs. These five business areas included: Debt Management Services, Federal Finance, Financial Operations, Information Resources, and Regional Operations.

We found that the FMS consolidated questionnaire, provided to GAO on September 26, 2001, did not always reflect the responses made by the subordinate business areas and that some of FMS' responses were incomplete and/or inconsistent with what our review determined. However, FMS officials stated that due to the general nature of the questionnaire and the lack of clarity, many of their responses were different from what our review disclosed.

Also, FMS stated that some questions were not applicable to FMS' system structure. For example:

- ***Question 16***. Question 16 asked whether FMS had a written policy that specifically addresses the handling of records that contain individuals' SSNs. FMS responded yes (for many programs). We found at the start of our review, that FMS did not have a written policy that addressed the handling of records that contain individual SSNs. In May 2002, FMS developed a draft policy that required all FMS employees to be aware of and follow the requirements of the Privacy Act and other applicable authorities and policies related to the collection, maintenance, use, and dissemination of personal information, including SSNs. The new Privacy Act policy, which was finalized in September 2002, also requires contractor and financial agency agreements to contain provisions pertaining to the third parties' responsibilities with regard to the use of personal information obtained from FMS and the training of employees of the third party.

- ***Question 19***. Question 19 asked how often FMS' list of employees with access to records that contain SSNs is updated. FMS responded that the process was performed once or twice a year, or as needed to reflect changes in employee assignments. We found that FMS does not periodically update its listings. A prior year finding reported that FMS failed to effectively manage and monitor access listing and users accounts. Additionally, we found that for most of FMS' automated information systems that we reviewed, FMS did not perform updates or re-certification procedures of user accounts on a periodic basis. FMS has a policy and procedures that require reviews and maintenance; yet, they were not followed. In July 2002, FMS updated the user access listings to satisfy a prior year audit finding. We noted that the July update did not include all FMS owned systems, e.g., agent operated systems or external users with access to FMS' systems. FMS informed us that revised policies for automated information systems accounts management and re-certification procedures were to be implemented in January 2003.

- ***Question 29***. Question 29 asked how often FMS tested the computer systems with SSNs stored to identify potential weaknesses that threaten security (risk assessments). FMS responded more than once a year (for some programs). Based on our review, we found that FMS had an adequate risk management policy. FMS' policy specifically states that a risk analysis process should be established and maintained. However, at the start of our review, when we requested risk assessments for the 27 systems, FMS provided business risk assessments for various business programs in which several of the 27 systems were identified as critical assets. FMS informed us that business risk assessments were not intended to replace the required computer system risk assessments. Upon completion of our fieldwork, FMS had only provided us with three computer risk assessments. FMS is currently working to develop computer system risk assessments for all of its systems as part of its certification and accreditation process.

- ***Question 32***. Question 32 asked how many separate computer systems FMS had with records that contain individuals' SSNs. FMS' initial response to GAO in September 2001 was at least nine. In June 2002, FMS confirmed that it had 24 systems with SSN records. Subsequently, in July 2002, FMS revised that number to 27 computer systems. FMS officials stated that they could not readily identify all of its systems that contain SSNs because they did not categorize their systems according to whether SSNs are included or not.

- ***Question 33***. Question 33 asked how many of the separate computer systems identified in question 32 have security plans. FMS left this question unanswered. We found that FMS had security plans for 21 of the 27 systems with SSNs records.

- ***Question 35***. Question 35 asked since the initial computer security plans were developed, how often have those plans been updated. FMS response was less often than once every two years. We found at the beginning of our review that most of the security plans had not been updated at all.

- ***Question 57***. Question 57 asked if a staff member in FMS had responsibility for determining which employees in other organizations will have access to individual SSNs stored in FMS computer systems. FMS response was no for most programs. We found that FMS external users must have an internal FMS sponsor submit a request for access on their behalf. This request must be documented electronically, appropriately approved, and retained in the file by the system owner staff.

FMS disagreed with our conclusion that some of its answers were incomplete and/or inconsistent with what our review determined. FMS officials stated that responses were based on their interpretations of the questions and that the answer choices were inflexible and written for an agency that operated a single program, rather than the multiple programs FMS operates. FMS officials also stated that GAO provided no guidance in writing, and little guidance in response to telephone inquiries on how to respond to the complex questionnaire for which agencies were given only 2 weeks to respond.

* * * * * *

We appreciate the cooperation and courtesies extended to our staff during the audit. If you have any questions, please contact me at (202) 254-4164, or a member of your staff may contact Lynn Richardson, Audit Manager at (202) 254-4226. Major contributors to this report are listed in *Appendix 4*.

Alexander Best, Jr.
National Director, Enforcement Program Audits

Our overall objective was to access FMS' controls over the access, disclosure, and use of SSN information by third parties. Our specific objectives were to determine whether FMS:

- Makes legal and informed disclosures of SSNs to third parties;
- Has appropriate controls over contractors' access and use of SSNs;
- Has appropriate controls over other entities' access and use of SSNs;
- Has adequate controls over access to individuals' SSNs maintained in its databases; and
- Has provided answers to GAO's questionnaire that were consistent with what our review determined.

FMS identified 27 automated information systems that contained SSNs. The 27 automated information systems did not include any systems in FMS' Management, Agency Services, or Governmentwide Accounting, Assistant Commissioner areas. These areas were not included in the scope of our audit.

Our review generally covered FY 2001. To accomplish our review, we reviewed applicable laws and regulations regarding the use and protection of SSNs and other sensitive information; FMS' policies, standards, and procedures; Memorandums of Understanding; Letters of Agreement; and other documentation related to the use, disclosure, and protection of SSNs. We also reviewed GAO reports, Clifton Gunderson reports, and FMS' self-assessments regarding safeguarding SSNs and other Privacy Act information.

We interviewed FMS and FRB officials responsible for controlling SSN access, use, and disclosure. We verified and updated key pieces of information provided on the GAO questionnaire. We conducted audit work at FMS Headquarters in Washington, D.C., and at its Hyattsville, Maryland location.

We conducted our audit between February 2002 and December 2002 in accordance with generally accepted government auditing standards.



COMMISSIONER

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

April 22, 2003

MEMORANDUM FOR ALEXANDER BEST, JR
NATIONAL DIRECTOR
ENFORCEMENT PROGRAM AUDITS

FROM: RICHARD L. GREGG

SUBJECT: Financial Management Service (FMS) Response to Draft Report on Review of FMS' Controls Over the Access, Disclosure, and Use of Social Security Numbers By Third Parties

Thank you for the opportunity to comment on the April 2, 2003, draft audit report entitled "Government-wide Financial Management Service: Review of FMS' Controls Over the Access, Disclosure, and Use of Social Security Numbers By Third Parties." We concur with the recommendations. Our efforts to address the audit findings have been on-going throughout the duration of this audit.

Information security has been a top priority for the Financial Management Service (FMS) in its mission of processing the vast majority of Government payments and collections, and managing the governmentwide collection of delinquent debt. Given the nature of our business, which requires us to process and handle sensitive personal information, the need to protect and restrict access to this information is ingrained in the FMS culture. It is important to note that no material problems were found at FMS involving the misuse or unauthorized disclosure of social security numbers, and that FMS continues to be committed to ensuring information security and privacy, as indicated by the myriad of controls that cover its activities.

As noted in the draft report, FMS has strengthened its privacy policies in numerous ways to ensure that any disclosures it makes of social security numbers to third parties are authorized and appropriate. Emphasis on continual improvement of FMS' control environment also resulted in important improvements being made last year to FMS' financial agency agreement/contract terms and conditions, information technology policies and standards, and general and application controls. In addition, FMS has immeasurably improved Treasury's protection of social security numbers that appear on Treasury checks. Treasury has taken the necessary steps to ensure that social security numbers are no longer visible through Treasury check window envelopes, and plans to remove the numbers from Treasury checks issued on or after January 1, 2004.

Page 2 – FMS Response to Draft Report Entitled Review of FMS' Controls Over the Access, Disclosure, and Use of Social Security Numbers By Third Parties

FMS remains committed to continuously strengthening its policies and procedures with respect to the protection of social security numbers. A detailed corrective action plan will be developed after a thorough analysis of the recommendations is completed. Our plan will consider all areas of FMS and include realistic timeframes for completing proposed actions. In the attachment, we have addressed each of the recommendations included in the report.

Attachment

cc. Donald Hammond

Attachment

Status of Actions

Finding 1

No recommendations.

Finding 2

The Commissioner should:

Recommendation 1: Strengthen written policies and/or procedures to:

a. Establish and administer programs with financial agents to ensure that all third party contractor and financial agent employees who have access or use SSN information in its automated systems are validated;

> **Response**: FMS has established the Bank Review Office to provide security oversight support for the Government-wide collections program. On-site security reviews are conducted of financial agents and contractor facilities. A critical function of these reviews is to ensure that financial agents have implemented effective security controls with respect to facilities, personnel and sensitive information associated with government collection activities, to prevent theft, compromise and unauthorized disclosure. **Completed**

b. Ensure that FMS finalize and implement the FMS Privacy Act clauses and provisions for agreements with the financial agents and that the FAR and FMS Privacy Act clauses are included in all applicable contracts and task orders.

> **Response**: In addition to using the Privacy Act clauses as listed in the Federal Acquisition Regulation (FAR) when appropriate, FMS drafted supplemental individual Privacy Act clauses to be used in FMS contracts and agreements, as applicable. FMS has implemented internal procedures to ensure that program staff inform its Acquisition Management Division (AMD) when a requirement includes Privacy Act concerns so that AMD can include the appropriate clauses in contracts and task orders. Privacy Act clauses are also incorporated into financial agency agreements when appropriate. Regarding the FMS task orders issued to private collection agencies, in addition to the appropriate FAR clauses contained in the General Services Administration contract, the FMS task orders executed in 2001 require the contractors to comply with the Privacy Act. The task orders also require contractors to train and certify employees on the Privacy Act. **Completed**

Recommendation 2: Ensure that FMS' agreements with credit bureaus are updated to conform to the Memorandum Of Understanding (MOU) contained in FMS' *Guide to the Federal Credit Bureau Program.*

Attachment

Response: FMS has updated six (6) of seven (7) required agreements with the credit bureaus used in its debt collection program to conform to the MOU contained in FMS' *Guide to the Federal Credit Bureau Program.* We are expecting the last agreement to be signed within the next week. If not received as promised, FMS will stop reporting consumer debt to the credit bureau that has failed to sign the necessary MOU.

.

Recommendation 3: Continue to monitor the activities of contractors, financial agents, and fiscal agents to ensure that sensitive information is safeguarded as required, including the requirement to conduct periodic independent third party reviews.

Response: FMS has established the Bank Review Office to provide security oversight support for the Government-wide collections program, and to ensure that an aggressive, proactive approach is taken to identify and address security weaknesses and instances of non-compliance with applicable Treasury directives/requirements. Federal Finance has implemented a policy to ensure that systems are subject to periodic independent third-party reviews. In addition to the unannounced security reviews at lockbox processing sites that have been conducted for several years, Federal Finance has also conducted such reviews at Ca$hLink and EFTPS sites, and has conducted security certification reviews at IRS lockbox processing sites. Federal Finance has also developed a comprehensive, automated system for reporting and tracking incidents, review findings, and corrective actions. **Completed**

Contractor adherence to the Privacy Act will be monitored and assessed as a contractor performance measure. As a matter of practice, both performance-based service contracts and nonperformance-based service contracts will reflect this as a performance measure and reporting requirement. FMS contractors will be assessed on this element in our past performance database. Debt Management Services and other areas will continue to monitor the activities of contractors to ensure that sensitive information is safeguarded. **Completed**

Recommendations 4: Modify security policies and standards dated June 26, 2002, to reflect the new requirements for Federal Reserve Banks (FRB) as fiscal agents.

Response: We are in the process of implementing this recommendation to modify FMS' existing security policies, standards, and procedures to reflect the correct requirements for the FRBs. FMS notes that there are no new requirements for FRBs. See page 11 of the Draft Report: "It is FMS' assessment that the Federal Reserve's Standards in this area more than meet the security goals of FMS. FMS officials reported in November 2002, that FMS' existing security policies, standards, and procedures would be revised to document the correct policy for the FRBs."

Attachment

Recommendation 5: Ensure that the new chapter of the Treasury Financial Manual (TFM) is revised and implemented as planned.

> **Response**: The new chapter of the TFM was published on March 4, 2003. The chapter reflects the existing practices of the FRBs with respect to the protection of information. **Completed**

Finding 3

The Commissioner should:

Recommendation 1: Ensure that all FMS business areas, fiscal agents, financial agents, and contractors adhere to its revised IT policies, standards, and procedures, dated June 2002, and any future revisions.

> **Response:** We are taking steps to implement this recommendation. Among other steps, Senior Executives are briefed monthly on IT security issues, concerns, or events. Further, the ongoing Certification and Accreditation effort will ensure adherence to IT policies, standards, and procedures.

Recommendation 2: Continue to improve its security planning process by ensuring that OMB and NIST guidelines are followed for all systems and major applications by:

a. Continuing to develop and/or revise the security plans for all systems in accordance with FMS and Federal guidelines.

> **Response:** FMS Security Plans are being reviewed and/or revised in 2003 as part of the certification process currently underway at FMS. Security Plans are currently being developed for all systems running at the Federal Reserve Banks.

b. Ensuring that security plans are established prior to the issuance of system certifications and accreditations.

Response: We are implementing this recommendation for all new systems. We are also updating and/or developing security plans for all operational systems.

c. Ensuring that system risk assessments are conducted for all systems.

> **Response:** FMS is completing system risk assessments in 2003 as part of the planned Certification and Accreditation process.

Recommendation 3: Fully implement the new computer security incident reporting guidelines and institute its computer incident reporting capability as planned.

> **Response:** We are in the process of implementing this recommendation.

Attachment

Recommendation 4: Improve monitoring of user access activities in systems that contain SSNs by:

a. Implementing re-certification user access procedures within its systems (including fiscal and financial operated systems) as scheduled.

> **Response:** We are in the process of implementing re-certification of all Enterprise users. The Check Payment & Reconciliation System (CP&R) and Intra-Governmental Payment and Collection (IPAC) System have re-certified users. The Treasury Offset Program (TOP) continues to review all users on a quarterly basis. All other applications will be recertifying users on an annual basis beginning in 2003.

b. Ensuring that all FMS operated systems are included in the FMS [redacted]

> **Response:** FMS is in the process of implementing the IBM Tivioli Identity Implementation (ITIM) product, which will replace the [redacted] ITIM will include all systems operating on the FMS Enterprise platform.

Recommendation 5: Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing access to the system.

> **Response:** In FY02 FMS employees received security awareness training and signed FMS' Rules of Behavior. Security training will occur annually. FMS requires that new employee training includes a session on employees' security responsibilities. As of October 2002, FMS also requires all new employees to sign FMS' Rules of Behavior prior to being granted access to FMS systems. **Completed**

Finding 4

No recommendations.

Enforcement Directorate

Alexander Best, Jr., National Director, Enforcement Program Audits
Lynn Richardson, Audit Manager
Irene Aultman, Auditor-In-Charge
Beverly Dale, Senior Auditor

U.S. Department of the Treasury

Fiscal Assistant Secretary
Director, Office of Strategic Planning and Evaluations
Director, Office of Accounting and Internal Control

Financial Management Service

Commissioner
Deputy Commissioner
Assistant Commissioner, Debt Management Services
Assistant Commissioner, Federal Finance
Assistant Commissioner, Financial Operations
Assistant Commissioner, Information Resources
Assistant Commissioner, Regional Operations
Audit Liaison

Office of Management and Budget

OIG Budget Examiner