



Audit Report



OIG-05-022

**GOVERNMENT-WIDE FINANCIAL MANAGEMENT SERVICES:
The Financial Management Service Has Addressed
Recommendations on Controls Over the Access, Disclosure, and
Use of Social Security Numbers by Third Parties
[Follow-Up on OIG-03-083]**

December 20, 2004

Office of
Inspector General

Department of the Treasury

Contents

Audit Report

| | |
|---|---|
| Results in Brief..... | 3 |
| Background | 3 |
| Finding | |
| FMS Has Addressed Recommendations | 4 |

Appendices

| | |
|---|---|
| Appendix 1: Objective, Scope, and Methodology | 6 |
| Appendix 2: Management Response | 8 |
| Appendix 3: Report Distribution..... | 9 |

Abbreviations

| | |
|-------|---|
| AC | Assistant Commissioner |
| AMS | Audit Monitoring System |
| FISMA | Federal Information Security Management Act |
| FMS | Financial Management Service |
| FY | Fiscal Year |
| IT | Information Technology |
| ITSOC | IT Security Oversight & Compliance Staff |
| JAMES | Joint Audit Management Enterprise System |
| MCB | Management Control Branch |
| OIG | Office of Inspector General |
| PCA | Planned Corrective Action |
| PCIE | President’s Council on Integrity and Efficiency |
| SSA | Social Security Administration |
| SSNs | Social Security Numbers |

*The Department of the Treasury
Office of Inspector General*

December 20, 2004

Richard L. Gregg
Commissioner
Financial Management Service

This report provides the results of an audit that followed up on an Office of Inspector General (OIG) audit report titled *FMS Continues To Improve Its Controls Over the Access, Disclosure, and Use of Social Security Numbers by Third Parties*, OIG-03-083. The objective of the audit was to determine the status of corrective actions taken by the Financial Management Service (FMS) in response to the 10 recommendations contained in the report, which was issued on May 20, 2003.

The audit was conducted in response to a request from the Social Security Administration (SSA) OIG, as a follow up to a President's Council on Integrity and Efficiency (PCIE) project performed under its leadership that led to the issuance of the original Treasury OIG audit report. During September 22, 2004, testimony before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, the SSA Acting Inspector General spoke of the PCIE report. Because of continuing interest in the use and protection of Social Security Numbers (SSNs), the Subcommittee requested the status of planned corrective actions at the 15 agencies participating in the initial review.

We performed our field work during November 2004 at FMS offices in Washington, D.C., and Hyattsville, MD. A more detailed description of our objective, scope, and methodology is included in Appendix 1.

Results in Brief

FMS has addressed the recommendations in report OIG-03-083. The recommendations were all closed by January 2004. Using an internal system, the responsible FMS staff tracked the status of the recommendations, monitoring progress on planned corrective actions and verifying that they were completed. The status of the recommendations was correctly reflected in the Department's tracking system.

In a memorandum dated December 16, 2004, responding to our draft report, the Acting Comptroller of FMS expressed a continued commitment to the protection of SSNs. This memorandum is included in Appendix 2.

Background

The overall objective of our prior audit was to assess FMS's controls over the access, disclosure, and use of SSNs by third parties. The audit considered the 27 automated information systems that contained SSNs at that time. Not included in the scope were any systems in the Agency Services, Governmentwide Accounting, or Management areas. The audit generally covered Fiscal Year (FY) 2001.

In our prior report, we concluded that while FMS had strengthened its Privacy Act Program to ensure that it made legal and informed disclosures of SSNs to third parties, opportunities existed to improve controls. Specifically, FMS needed to better document, maintain, and monitor third party agreements to ensure that security requirements were met. FMS also needed to strengthen its general security controls over Information Technology (IT) applications and systems. As part of these security controls, FMS needed 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 employee access to computerized records; and (6) IT application and system training.

The report contained 10 recommendations to improve FMS's controls over the access, disclosure, and use of SSNs by third parties. FMS concurred with the recommendations. At the time that the report was issued, during May 2003, FMS had taken or planned to take corrective actions that the OIG determined addressed the intent of the recommendations.

Finding

FMS Has Addressed Recommendations

FMS has taken the planned corrective actions (PCA) to address the 10 recommendations in the prior OIG report. The recommendations were all closed in the July 2003 to January 2004 time frame, with completion of the PCAs being verified by the responsible FMS staff. The Joint Audit Management Enterprise System (JAMES) correctly reflected the status of the recommendations.

In determining the scope of our review, we considered the effectiveness of FMS's monitoring of audit recommendations. We found that there was a process in place to ensure that recommendations were addressed in a timely manner. Specifically, the Management Control Branch (MCB) coordinates the development of the FMS response to audit findings and recommendations, which includes the preparation of a corrective action plan. MCB desk officers ensure the proper recording, tracking, and monitoring of PCAs. In addition, the status of PCAs is discussed at monthly FMS Executive Board meetings, and revisions to agreed-upon target dates for completion require the written approval of the Commissioner or Deputy Commissioner.

At a Departmental level, the status of audit recommendations is tracked in JAMES. At a bureau level, FMS uses the Audit Monitoring System (AMS), which provides more flexibility and detailed day-to-day information. Verification of completion of the PCAs is performed by the MCB, except for matters dealing with IT,

which are verified by the IT Security Oversight & Compliance Staff (ITSOC). The only exceptions are cases where ITSOC is responsible for implementing IT-related PCAs. In these cases, in consideration of proper separation of duties,¹ MCB does the verification.

We found that, for each PCA that we reviewed, the records maintained by MCB and/or ITSOC contained evidence that completion of the action had been verified. Supporting documentation, consisting of such items as procedural issuances and staff sign-in sheets for training, was also maintained. There was evidence that training had been provided in areas such as IT security and certification and accreditation. This evidence included copies of the presentations. The files also contained signed copies of the *FMS IT Rules of Behavior*, which management stated had been handed out and discussed during training sessions. In addition, there was evidence that security plans were established as required for new systems processing SSNs; that risk assessments or self-assessments had been completed; and that security incident response guidelines were implemented.

* * * * *

We would like to extend our appreciation for the cooperation and courtesies extended to our staff during the review. If you have any questions, please contact me at (202) 927-6512 or Maria V. Carmona, Audit Manager, at (202) 927-6345. The major contributors to this report were Ms. Carmona and Dwight Glenn, Auditor.

Donald R. Kassel
Director, Banking and Fiscal Service Audits

¹ MCB is part of the Program Integrity Division, which reports to the Assistant Commissioner (AC) for Management, Chief Financial Officer. ITSOC is part of Mission Assurance, which reports to the AC for Information Resources, Chief Information Officer.

The audit objective was to determine the status of the 10 recommendations contained in an OIG audit report titled *FMS Continues To Improve Its Controls Over the Access, Disclosure, and Use of Social Security Numbers by Third Parties*, OIG-03-083, which was issued on May 20, 2003.

The scope of this follow-up audit was limited to the corrective actions planned by FMS in response to recommendations made in report OIG-03-083. The OIG had accepted the corrective actions as proposed by FMS. The prior report stated in each case that the proposed action(s) addressed the intent of the recommendation.

We met with managers and staff from the Program Integrity Division, the Management Control Branch, Mission Assurance, and the IT Security Oversight & Compliance Staff to (1) obtain an understanding of the process FMS uses to monitor the status of recommendations and (2) determine the status of each of the 10 audit recommendations. We reviewed how the status of each recommendation was reflected in the audit monitoring systems of the Department (JAMES) and FMS (AMS). We also reviewed the records maintained to document FMS's own verification of the completion of PCAs. In addition, we considered work performed at FMS by other Treasury OIG auditors and contractors as part of the FY 2003 and FY 2004 Federal Information Security Management Act (FISMA) reviews.

We verified completion for a sample of PCAs. Our review determined if a PCA had been taken, but was not intended to be a comprehensive review of the validity and effectiveness of the action. For example, if a PCA stated that a security plan would be developed for a specific system, we confirmed that a security plan had been prepared and reviewed the plan, but did not perform an in-depth analysis of the security plan.

The prior OIG audit report had four findings, two of which (Findings 1 and 4) did not include any recommendations. The other two findings had five recommendations each, for which FMS identified 28 PCAs. We selected a judgmental sample of five recommendations for review, as indicated by the shading in the Table below, and reviewed the documentation maintained as verification of completion of each of the corresponding 19 PCAs.

Table: Sample Selected for Review

| Finding 2 | | Finding 3 | |
|------------------|------------------|------------------|------------------|
| Rec. # | # of PCAs | Rec. # | # of PCAs |
| 1 | 8 | 1 | 1 |
| 2 | 2 | 2 | 6 |
| 3 | 3 | 3 | 1 |
| 4 | 3 | 4 | 2 |
| 5 | 1 | 5 | 1 |

We conducted our audit during November 2004 at FMS offices in Washington, D.C., and Hyattsville, MD, in accordance with generally accepted government auditing standards.

Appendix 2
Management Response



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

DEC 16 2004

MEMORANDUM FOR DONALD R. KASSEL
DIRECTOR, BANKING AND FISCAL SERVICE AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: KENT KUYUMJIAN 
ACTING COMPTROLLER

SUBJECT: Financial Management Service (FMS) Response to Draft Report
on the Follow-Up Review on Access, Disclosure, and Use of
Social Security Numbers by Third Parties

Thank you for the opportunity to comment on the December 10, 2004, draft audit report entitled "The Financial Management Service Has Addressed Recommendations on Controls Over the Access, Disclosure, and Use of Social Security Numbers by Third Parties [Follow-Up on OIG003-083]". We appreciate the opportunity to work with your staff on this audit and are pleased with the results of your review. We will continue to give considerable thought and effort into the protection from third parties of social security numbers for all systems in operation and under development in the FMS network. FMS has no additional comments on this audit.

Department of the Treasury

Fiscal Assistant Secretary
Office of Strategic Planning and Performance Management
Office of Accounting and Internal Control

Financial Management Service

Commissioner
Deputy Commissioner
Director, Program Integrity Division
Manager, Management Control Branch

Social Security Administration

Office of Inspector General

Office of Management and Budget

OIG Budget Examiner