SOCIAL SECURITY

February 28, 2005

The Honorable Adam Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives
Washington, D.C. 20515

Dear Mr. Putnam:

During testimony on September 22, 2004 before your Subcommittee, I discussed Federal agencies' use of Social Security numbers. As part of this discussion, I mentioned the 2003 President's Council on Integrity and Efficiency report, *Federal Agencies' Controls over the Access, Disclosure and Use of Social Security Numbers by External Entities*. Because of your continuing interest in the use and protection of Social Security numbers, we conducted a follow-up review to determine the status of corrective actions Federal agencies have taken to address recommendations resulting from this review. The enclosed report summarizes the results of our review.

If you have any questions or would like to be briefed on this issue, please call me or have your staff contact H. Douglas Cunningham, Assistant Inspector General for Congressional and Intra-Governmental Liaison, at (202) 358-6319.

Sincerely,

Patrick P. O'Carroll, Jr.
Inspector General

Enclosure

cc:
Jo Anne B. Barnhart

CONGRESSIONAL RESPONSE REPORT

Follow-up of Federal Agencies' Controls over the Access, Disclosure, and Use of Social Security Numbers by External Entities

A-08-05-25101

February 2005

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the Congress, and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

Background

OBJECTIVE

During testimony on September 22, 2004 before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, we discussed Federal agencies' use of Social Security numbers (SSN). As part of the discussion, the Acting Inspector General mentioned the 2003 President's Council on Integrity and Efficiency (PCIE) report, *Federal Agencies' Controls over the Access, Disclosure and Use of Social Security Numbers by External Entities*. Because of continuing interest in the use and protection of SSNs, we conducted a follow-up review to determine the status of corrective actions Federal agencies have taken to address recommendations resulting from this review.

BACKGROUND AND GENERAL DESCRIPTION

The SSN was created in 1936 as a means of establishing and maintaining 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.

Although no single Federal law regulates the 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 (see Appendix A). In addition, a number of Federal laws lay out a framework for Federal agencies to follow when they establish information security programs that protect sensitive personal information, such as SSNs.[1]

The expanded use of the SSN as a national identifier provides a tempting means for many unscrupulous individuals to acquire an SSN and use it for illegal purposes. While no one can fully prevent SSN misuse, Federal agencies have some responsibility to limit the risk of unauthorized disclosure of SSNs. Because of concerns related to sharing of personal information and occurrences of identity theft, in 2002, Congress asked that we look at how Federal agencies disseminate and control the use of SSNs. After consulting with the PCIE, we agreed to serve as lead for 15 participating Offices of Inspector General (OIG) and prepare the final report (see Appendix B). Most OIGs issued reports to their respective departments or agencies that included recommendations for corrective actions. Each OIG focused its work on one program

[1] *See* National Defense Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398, § 1061, 114 Stat. 1654 (2000); National Defense Authorization Act for Fiscal Year 1996, Pub. L. No. 104-106, § 2(a)(4) and (5), 110 Stat. 186 (1996); the Paperwork Reduction Act of 1995, Pub. L. No. 104-13, 109 Stat. 163 (1995); the Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988). *See also* Office of Management and Budget Circular A-130, *Management of Federal Information Resources* (November 28, 2000).

within its respective agency.[2] As such, we concluded that any findings should not be extrapolated to all programs in each agency. See Appendix C for the specific program each OIG reviewed.

This report serves as a follow up to the 2003 PCIE report, *Federal Agencies' Controls over the Access, Disclosure and Use of Social Security Numbers by External Entities.* In performing this review, we requested that each OIG provide us the status of corrective actions taken by their respective agency to address recommendations resulting from the previous review. We did not request that each OIG determine whether their respective agency was still at-risk for improper access, disclosure and use of SSNs by external entities. As such, this report provides examples of some corrective actions taken by Federal agencies and does not address whether the agencies have adequate SSN controls. We conducted our review in accordance with the PCIE's *Quality Standards for Inspections*.

[2] The Department of Defense assessed SSN controls for three programs.

Results of Review

In 2003, most OIGs reported their respective agencies had inadequate controls over the access, disclosure and use of SSNs by external entities. Of the 15 agencies reviewed,

- 14 lacked adequate controls over contractors' access to, and use of, SSNs;
- 9 had inadequate controls over the access to SSNs maintained in their computer systems;
- 2 did not have adequate controls over non-Government and/or non-contractor entities' access to, and use of, SSNs; and
- 1 did not make legal and informed SSN disclosures.

We concluded that Federal agencies would benefit by strengthening some of their controls over the access, disclosure and use of SSNs by external entities. We are encouraged to learn that all 15 Federal agencies have taken corrective actions to strengthen some of their SSN controls.

CONTRACTORS' ACCESS TO, AND USE OF, SSNs

Federal agencies incorporate different practices to ensure they have appropriate controls over contractor access to, and use of, SSNs. These include, but are not limited to, passwords and computer identifications; access to information on a need-to-know basis; periodic review of current computer users; staff and contractor confidentiality agreements; security awareness training; and secure work areas. Despite these safeguard requirements, 14 (93 percent) of 15 OIGs previously reported their respective agency had inadequate controls over contractors' access to, and use of, SSNs (see Appendix C).

As illustrated in the following examples, all of the 14 Federal agencies have taken some actions to address the vulnerabilities identified.[3]

- Eight OIGs reported their agencies performed site inspections to ensure contractors upheld their obligation to protect the confidentiality and security of SSNs.
- Four OIGs reported their respective agencies provided employees and contracting officers security awareness and/or Privacy Act training.
- One OIG reported its agency added audit steps for selected reviews to test contractors' procedures for safeguarding individuals' personal identifying information, such as SSNs.

[3] Because some OIGs reported their agencies have taken multiple corrective actions, the number of examples exceeds the number of Federal agencies.

- Another OIG reported its agency reviewed contractors' security plans and includes non-agency employees who have access to agency computer systems in its annual security audit.

- Another OIG reported its agency requires that new employees and contractors complete an *Information Technology Access Request Form* to gain access to the agency's mainframe. This agency also established controls to ensure it deletes contractors' systems access after they leave the agency.

ACCESS TO INDIVIDUALS' SSNs MAINTAINED IN AGENCY DATABASES

In the 2003 review, Federal agencies that allowed access to their databases generally had standard information security controls in place. Agency controls included, but were not limited to, security clearances before granting computer access, computer access controlled by job title, unique user identification and passwords, firewalls, encrypted data transportation, intrusion detection systems, and physical access controls. Despite these safeguards, 9 (60 percent) of 15 OIGs reported their respective agencies had inadequate controls over access to SSNs maintained in their databases. Because of the sensitive nature of information security issues, we chose to withhold detailed descriptions of information security control weaknesses identified by OIGs (see Appendix C).

As illustrated in the following examples, all of the nine Federal agencies have taken actions to address these control weaknesses.

- One OIG reported its agency instructs all system users to ensure contractors are aware of agency policies and procedures and Federal laws prohibiting the disclosure of SSN information. This agency removes the system user's access upon receipt of the user's termination letter and requires that each system user have security clearance at a level commensurate with their duties.

- Another OIG reported its agency revised its computer access forms to identify the user's security level and access needs. All of the agency's forms include the statement, "Any screen or printout displaying names and SSNs contains confidential information that must be secure."

NON-GOVERNMENT/NON-CONTRACTOR ENTITIES' ACCESS TO, AND USE OF, SSNs

In the 2003 review, 2 (13 percent) of 15 OIGs reported their agencies did not have adequate controls over non-Government/non-contractor entities' access to, and use of, SSNs. One OIG reported its agency had no standard contract language to include Privacy Act safeguards. Another OIG reported its agency had not established financial standards for outside parties to meet before accessing data containing SSN information (see Appendix C).

As illustrated in the following examples, these Federal agencies have taken some actions to address the vulnerabilities identified.

- One OIG reported its agency established standards for safeguarding SSNs. In addition, the agency incorporated security features into all phases of its information technology acquisition process and established security requirements for third parties who wish to contract with the agency to provide automated data processing services.

- The other OIG reported its agency developed a cover letter that it sends to independent physicians encouraging them to comply with the principles of the Privacy Act.

DISCLOSURES OF SSNs TO EXTERNAL ENTITIES

In the 2003 review, 1 (7 percent) of 15 OIGs reported its agency did not make legal and informed SSN disclosures (see Appendix C). This OIG identified instances in which the agency did not inform research study participants that providing their SSNs was voluntary. This OIG recommended that its agency establish guidelines to ensure confidentiality of SSNs. The agency revised a staff manual that addresses handling private information, such as SSNs. The manual states that all contractors are responsible for strictly adhering to the procedures established in agency guidelines. It also requires that management conduct periodic inspections of contractor sites and that all contract employees sign an agreement for the protection of private information.

Although the 14 remaining OIGs reported their agencies generally made legal and informed SSN disclosures,[4] they identified instances in which agency practices increased the risk that external entities may have improperly obtained and misused SSNs. One OIG identified instances in which its agency unnecessarily displayed SSNs on documents it sent to external entities that may not have had a need to know. Another OIG identified instances in which its agency inadvertently omitted the Privacy Act notice on one of its forms. The following examples illustrate some of the corrective actions taken by Federal agencies.

- One OIG reported its agency established new policies to limit the display of SSNs on correspondence.

- Another OIG reported its agency revised one of its forms to include the Privacy Act notice.

[4] For purposes of this report, we consider SSN disclosure to have occurred when an agency provides an SSN to an external entity that did not already have it.

Conclusions

We previously reported that some Federal agencies were at-risk for improper access, disclosure and use of SSNs by external entities, despite safeguards to prevent such activity. As such, we concluded that Federal agencies would benefit by strengthening some of their SSN controls. We are encouraged that all OIGs reported their respective agencies have taken some corrective actions to strengthen controls over the access, disclosure and use of SSNs by external entities. Given the potential for individuals to improperly obtain and misuse SSNs, we encourage Federal agencies to continue their efforts to safeguard SSNs.

Appendices

Federal Laws that Restrict Disclosure of the Social Security Number

The following Federal laws establish a framework for restricting Social Security number (SSN) disclosure.[1]

The Freedom of Information Act of 1966 (5 U.S.C. § 552)

The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of Executive Branch agencies and departments are accessible to the people. FOIA, as amended, provides that the public has a right of access to Federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the Government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to State and local governments.

The Privacy Act of 1974 (5 U.S.C. § 552a)

The Privacy Act regulates Federal agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records. The Act prohibits the disclosure of any record contained in a system of records unless the disclosure is made based on a written request or prior written consent of the person to whom the records pertain, or is otherwise authorized by law. The Act authorizes 12 exceptions under which an agency may disclose information in its records.

The Act contains a number of additional provisions that restrict Federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or Executive Order of the President, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under Federal programs.

[1] Summarized from *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

The Social Security Act Amendments of 1990 (42 U.S.C. § 405(c)(2)(C)(viii))[2]

The Social Security Act bars disclosure by Federal, State and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the Act also contains criminal penalties for "unauthorized willful disclosures" of SSNs. Because the Act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by Federal entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear if the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to Federal, State and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

[2] Pub. L. No. 101-624, §2201, 104 Stat. 3359, 3951 (1990).

Participating Offices of Inspector General

Department of Agriculture

Department of Defense

Department of Education

Department of Health and Human Services

Department of Housing and Urban Development

Department of Labor

Department of the Treasury

Environmental Protection Agency

Federal Deposit Insurance Corporation

Nuclear Regulatory Commission

Office of Personnel Management

Railroad Retirement Board

Small Business Administration

Social Security Administration

Treasury Inspector General for Tax Administration

Summary of Inadequate Controls Identified by Offices of Inspector General (OIG)

Federal Agency and Program(s) Reviewed	INADEQUATE CONTROLS IDENTIFIED BY OIGs			
	Contractor Access and Use of SSNs	Access to SSNs Maintained in Agency Databases	Non-Government/ Non-contractor Access and Use of SSNs	Legal and Informed Disclosure of SSNs to External Entities
Department of Agriculture: Food Stamp Program	X[1]	X[1]		
Department of Defense: Defense Manpower Data Center; Army and Air Force Exchange Service, and Defense Security Service	X[2]	X[3]		
Department of Education: Pell Grant Program	X	X		
Department of Health and Human Services: Food and Drug Administration	X			X
Department of Housing and Urban Development: Office of Housing	X			

[1] Inadequate controls identified at the State/local levels of the Food Stamp Program.

[2] Inadequate controls over contractor access and use of SSNs identified in the following Department of Defense agencies: Army and Air Force Exchange Service and Defense Security Service.

[3] Inadequate controls over access to SSNs maintained in its databases identified at the Defense Manpower Data Center.

Federal Agency and Program(s) Reviewed	Inadequate Controls Identified by OIGs			
	Contractor Access and Use of SSNs	Access to SSNs Maintained in Agency Databases	Non-Government/ Non-contractor Access and Use of SSNs	Legal and Informed Disclosure of SSNs to External Entities
Department of Labor: Federal Employee Compensation Act Program	X		X	
Department of the Treasury: Financial Management Service	X	X		
Environmental Protection Agency: Financial Management and Financial Services Divisions				
Federal Deposit Insurance Corporation	X		X	
Nuclear Regulatory Commission	X	X		
Office of Personnel Management: Retirement and Insurance Service, Office of Merit Systems Oversight and Effectiveness, and Investigations Service	X	X		
Railroad Retirement Board	X	X		
Small Business Administration	X			
Social Security Administration: Title II Program	X	X		
Treasury Inspector General for Tax Administration: Internal Revenue Service	X	X		
TOTALS	**14**	**9**	**2**	**1**

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations,
House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Executive Operations (OEO). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Executive Operations

OEO supports OIG by providing information resource management and systems security. OEO also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OEO is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.