SOCIAL SECURITY

MEMORANDUM

Date: August 19, 2004 Refer To:

To: The Commissioner

From: Acting Inspector General

Subject: The Social Security Administration's Internal Use of Employees' Social Security Numbers (A-13-04-24046)

The attached final report presents the results of our audit. Our objectives were to determine the extent of the Social Security Administration's internal use of employees' Social Security numbers (SSN) and to evaluate the safeguards used within the Agency to protect the confidentiality of these SSNs.

Please provide within 60 days a corrective action plan that addresses each recommendation. If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S INTERNAL USE OF EMPLOYEES' SOCIAL SECURITY NUMBERS

August 2004 **A-13-04-24046**

AUDIT REPORT

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.

Executive Summary

OBJECTIVE

Our objectives were to determine the extent of the Social Security Administration's (SSA) internal use of employees' Social Security numbers (SSN), and to evaluate the safeguards used within the Agency to protect the confidentiality of these SSNs.

BACKGROUND

The SSN was created in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. Nevertheless, over the years, the SSN has become a de facto national identifier used by Federal agencies, State and local governments, and private organizations. The expanded use of the SSN as a national identifier provides a tempting motive for unscrupulous individuals to acquire an SSN and use it for illegal purposes.

Federal agencies frequently ask individuals for their SSNs because, in certain instances, the law requires that they do so or SSNs provide a convenient means of tracking and exchanging information. Federal agencies have a responsibility to limit the risk of unauthorized disclosure of SSNs. 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.

RESULTS OF REVIEW

The SSN is used extensively within SSA's systems and documents to identify its employees. Further, SSA has some safeguards in place to protect the confidentiality of its employees' SSNs. However, SSA needs to enforce current policies to ensure SSA employees' SSNs are protected.

CONCLUSION AND RECOMMENDATIONS

SSA's extensive use of employee SSNs in its systems and documents increases the risk that the employee SSN may be accessed by unauthorized personnel. SSA has mitigated this through some safeguards, but additional actions are needed. With the increasing impact of identity theft on the public and economy, and as the issuer of SSNs, SSA should be the model for both the public and private sectors by taking the leadership role in protecting SSNs, including those of its employees.

We recommend SSA:

- Remind employees to secure any system or document containing employee SSNs when these systems or documents are not being used.

- Consider using asterisks, if determined to be cost-effective, to hide the employee SSN on computer screens and reports in all existing and future systems. Asterisks are currently used in the Mainframe Time and Attendance System to hide the employee SSN.

- Identify the forms that request the employee's SSN. If the SSN is not required, eliminate its use on these forms.

- Determine if it is cost beneficial to use an alternative primary identifier for its employees, such as the one used in the *On-Line University*, for all future SSA systems. If determined to be cost-beneficial, then implement an alternative primary identifier.

- Consider and use, as indicated in Agency policy, encryption if feasible and not cost prohibitive.

AGENCY COMMENTS

SSA agreed with our recommendations. Further, the Agency agreed that it needed to exercise due diligence in protecting employee SSNs. The Agency noted that unlike the private sector, it is bound by Executive Order 9397 and the 1961 Civil Service Commission directives, which mandate the use of SSNs as the identifier of Federal employees. As a result, the Agency states that until such time as both directives are rescinded or modified, it is required to use the SSN as the employee identifying number.

Also, in its response to Recommendation 5, the Agency believes it is already in compliance with the intent of our recommendation. The Agency indicates the use of dedicated lines and Connect Direct when transmitting payroll information to the Department of Interior complies with its policy concerning the transmission of sensitive data outside the Agency. The text of SSA's comments is included in Appendix D.

OIG RESPONSE

We agree the Agency is in compliance with its policy concerning the transmission of sensitive data outside the Agency. Additionally, we agree the use of dedicated lines, Connect Direct, or other secure transport mechanism(s) will provide some level of security for the transmitted data. However, we believe the Agency should also encrypt this sensitive data when transmitted outside the Agency. Data encryption would provide an additional level of security.

Table of Contents

Introduction

OBJECTIVE

Our objectives were to determine the extent of the Social Security Administration's (SSA) internal use of employees' Social Security numbers (SSN) and to evaluate the safeguards used within the Agency to protect the confidentiality of these SSNs.

BACKGROUND

The SSN was created 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. The expanded use of the SSN as a national identifier provides a tempting motive for unscrupulous individuals to acquire an SSN and use it for illegal purposes.

Federal agencies frequently ask individuals for their SSNs because, in certain instances, the law requires that they do so or SSNs provide a convenient means of tracking and exchanging information. While a number of laws and regulations require the use of SSNs for various Federal programs, they generally also impose limitations on how those SSNs may be used. Federal agencies have a responsibility to limit the risk of unauthorized disclosure of SSNs. Although no single Federal law regulates overall use and disclosure of SSNs by Federal agencies, the Freedom of Information Act of 1966,[1] the Privacy Act of 1974,[2] and the Social Security Act Amendments of 1990 generally govern disclosure and use of SSNs.

Federal Trade Commission Survey on Identity Theft

According to the Federal Trade Commission's (FTC) September 2003 survey report on identity theft "…a total of 4.6 percent of survey participants indicated that they had discovered they were victims of identity theft in the past year."[3] The report also indicated the results of the survey suggest almost 10 million Americans have discovered that they were victims of some form of identity theft within the last year.[4]

---

[1] The Freedom of Information Act, 5 U.S.C. § 552.
[2] The Privacy Act of 1974, 5 U.S.C. § 552a.
[3] *FTC – Identity Theft Survey Report*, September 2003. The report, which interviewed 4,057 U.S. adults, was prepared by Synovate, a research firm hired by the FTC. Identity theft occurs when someone uses your personal information, such as your name, SSN, credit card number or other identifying information, without your permission to commit fraud or other crimes. The FTC website: http://www.consumer.gov/idtheft/.
[4] id.

It was estimated that within the last 5 years, approximately 27 million Americans were victims of identity theft.[5] The total loss to businesses last year due to identity theft was nearly $48 billion, and the loss to consumers was $5 billion.[6]

Applicable Federal Criteria

Executive Order 9397, which provides SSA the authority to request an individual's SSN, states, "…whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize exclusively the Social Security Act account number."[7] Moreover, the Privacy Act of 1974 requires that SSA "…maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President."[8]

Further, the Privacy Act of 1974 regulates Federal agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records.[9] It requires agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity, which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

The Social Security Board – Regulation Number 1 states, "It being found by the Social Security Board that the public interest and the efficient administration of the functions with which the Board is charged under the Social Security Act require that the confidential nature of all wage records and other records or information in possession of the Board, pertaining to any person, be preserved."[10]

SSA policy states that an approach must be taken "…to ensure personal data entrusted to SSA is not compromised, abused or misused by the public or our own employees."[11] For additional background information, see Appendix B.

---

[5] id.
[6] id.
[7] Executive Order 9397, November 22, 1943.
[8] 5 U.S.C. § 552a.
[9] A system of records is a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
[10] Social Security Board Regulation Number 1, adopted June 15, 1937.
[11] Social Security Administration Information Systems Security Handbook, Chapter 1, February 2001.

Results of Review

The SSN is used extensively within SSA's systems and documents to identify its employees. Further, SSA has some safeguards in place to protect the confidentiality of its employees' SSNs. However, SSA needs to enforce current policies to ensure SSA employees' SSNs are protected.

SSNs ARE USED EXTENSIVELY BY SSA TO IDENTIFY ITS EMPLOYEES

The SSN is used extensively within SSA's systems and documents to identify its employees. The SSN is used as the primary identifier for employees in SSA's travel, training, time and attendance, and other human resources management information systems and documents.[12] For example, the SSN is used in SSA's Human Resources Management Information System (HRMIS)[13] to identify its employees' personnel actions, and in the Mainframe Time and Attendance System (MTAS) for processing employee pay and leave information. Employee SSNs are also used on SSA forms, such as *Training Nomination and Authorization*, *Travel Voucher*, and *Administrative Time and Leave Record*.[14] Additionally, the employee SSN is requested on various Office of Personnel Management (OPM) forms.[15] These forms are pre-approved by OPM and are used to add and update employee personnel records.

Further, SSA transmits data containing employee SSNs outside the Agency. SSA personnel stated that the employee SSN is required to interface with other agencies' computer systems. For example, SSA transmits employee payroll information to the Department of Interior (DOI)[16] and employee benefit program changes to the OPM using SSNs to identify employees.

[12] *Travel Manager*, Version 8.1, The Office of Training data, and the Agency's Mainframe and Attendance System all use employee SSNs as the primary identifier.
[13] HRMIS is a database that is used for multiple purposes to include personnel research and program evaluation, management information, equal opportunity statistics, and internal and external reporting.
[14] SSA352-U10 (*Training Nomination and Authorization*), SF 1012 (*Travel Voucher*), and SSA 2042 (*Administrative Time and Leave Record*).
[15] Examples of OPM approved forms are "Health Care Election Form" (SF 2809), and "Request for Personnel Action" (SF 52).
[16] DOI's Payroll Operations Division provides payroll services for several Government agencies including SSA.

SSA's extensive use of employee SSNs in its systems and documents increases the risk that the employee SSN may be accessed by unauthorized personnel. Therefore, the Agency must have the appropriate and cost-effective safeguards in place to protect the confidentiality of its employees' SSNs.

SSA HAS IMPLEMENTED SOME SAFEGUARDS TO PROTECT THE CONFIDENTIALITY OF ITS EMPLOYEES' SSNs

SSA has some safeguards in place to protect the confidentiality of its employees' SSNs. During our review, we observed security controls[17] for many of SSA's systems and documents that contain Agency employees' SSNs. These systems and documents contain sensitive information.[18] For example, HRMIS and MTAS require employees to obtain multiple levels of management approval[19] before being granted access to these applications. Further, MTAS will not display the employee's SSN on computer screens or printed reports.[20]

Moreover, these human resources management information systems require users to obtain personal identification numbers and passwords. Personal identification numbers and initial passwords are provided by SSA. Users' passwords are encrypted, and users are required to change their password at least every 30 days. If an individual should obtain unauthorized system access, certain systems produce violation reports, which are reviewed by SSA management.

In addition to safeguarding data contained in its systems, the Agency is required to safeguard the confidentiality of sensitive information it transmits to other Federal, State, and local governments. SSA policy states, "…in all instances where SSA data is transmitted outside of SSA, encryption must be considered and used if feasible and not cost prohibitive."[21]

---

[17] Security controls refer to policies and measures that ensure confidentiality, integrity, and availability of the information processed and stored by a computer. For example, physical security controls concerns the use of locks, guards, badges, alarm systems, and related administratively controlled measures to protect a structure or facility against unauthorized entry and measures to detect and minimize damage from accident, fire and environmental hazards.

[18] Sensitive information refers to information, the loss or misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled to under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. For example, SSA's employees' Social Security number, address, and birth date.

[19] Forms SSA-613-U5, *Top Secret Resource Access Authorization*, and SSA-120-U3, *Application for Access to SSA Systems* must be completed and management approved.

[20] Asterisks are used to denote employee SSNs.

[21] SSA Information Systems Security Handbook, Appendix H, September 2003. Encryption denotes conversion of a plain text, formula, combination or entry code into unintelligible form through the use of algorithms and keys. Encryption may be performed either by hardware or software.

We also observed physical security controls within several SSA components. Most of the areas observed were secure. The rooms and cabinets were locked. These rooms and cabinets house documents containing sensitive information including SSA employees' SSNs.

Besides the physical and computer security controls, SSA also has a computer security awareness program. The Computer Security Act of 1987[22] requires every Federal agency to provide periodic training in computer security awareness and security practices for all employees involved with the management, use, or operation of computers within the agency. SSA has developed a security awareness, training, and education program to assist management in complying with the Computer Security Act. SSA distributes pamphlets, Commissioner's bulletins, desk-to-desk bulletins, and videos to enhance employee security awareness.

We discussed with SSA management the possibility of eliminating the use of the employee SSN as a primary identifier in Agency systems and forms. SSA management stated it would not be cost-effective to eliminate the SSN in its existing systems. Further, SSA management noted many of its forms that require the SSN are mandated by OPM. Agency management explained it would be cost prohibitive to change its existing systems to enable the use of another primary identifier instead of the SSN. However, there have been no studies reflecting the cost of updating SSA's existing systems.

Although SSA management rejects the elimination of the SSN as a primary identifier, the Agency has taken steps to reduce its use of employees' SSNs. For example, some SSA managers encourage employees not to provide their SSN on leave slips and timesheets. Both of these forms request the employee SSN, but the employees' SSNs are not necessary for processing these forms. Additionally, SSA has developed certain systems that allow employees to process personal information without supplying their SSN. For example, SSA's "On-Line University" system uses the SSN to interface with HRMIS. However, SSA's "On-Line University" system allows SSA employees to use a unique identifier other than the SSN, to enroll in on-line training courses.

We believe the safeguards implemented by the Agency lowers the risk that the employee SSN may be compromised. Nevertheless, SSA needs to enforce its policies to ensure the employee SSN is protected.

[22] Public Law 100-235.

SSA NEEDS TO ENSURE POLICIES PROTECTING EMPLOYEES' SSNs ARE BEING ENFORCED

Although SSA has some policies in place to protect the confidentiality of its employees' SSN, additional enforcement of these policies is needed. During our review, we observed documents containing employees' SSNs filed in unlocked cabinets, which could be accessed by unauthorized personnel. For example, an Automated Clearing House report, which contains employees' SSNs, bank account numbers, bank routing numbers, and employee names, was stored in an unlocked file cabinet in an unlocked area. We visited the unsecured area after normal duty hours[23] and accessed the report from the file cabinet. In addition, we found other employee files containing sensitive employee information in unlocked cabinets in an unlocked room. We were able to access these files while employees were working in the area.

Further we observed, on several occasions, documents containing employee SSNs lying on tables. These documents contained employee SSNs and Internal Revenue Service wage information. We also observed information on computer screens which contained employees' SSNs. Occasionally, this information was printed and faxed to employees. For example, an employee can request travel status information, which is printed from a computer screen and faxed to the employee. This creates a risk that unintended employees may have access to an employee's SSN.

We also found instances where the employee SSN is requested on various forms.[24] Although SSA is limited in its ability to eliminate the SSN on many forms, we believe SSA has an opportunity to work within existing laws, regulations, and policies to identify and eliminate the SSN on forms where the SSN is not required. Further, we observed invoices from an external entity, which displayed SSA employee names, addresses and SSNs.

Through discussions with staff in the Office of Telecommunications and Systems Operations, Division of Network Engineering, we determined not all sensitive data transmitted externally to other entities are encrypted. SSA transmits employee payroll information to the DOI. However, those data are not encrypted. Staff in the Office of Telecommunications and Systems Operations explained they are investigating whether DOI has the software to facilitate the transmission of encrypted data between SSA and DOI.

We believe these deficiencies are potential security risks. Employees who do not have a "need to know"[25] may have access to sensitive employee information including the SSN. This information may be used by unscrupulous employees to acquire an SSN and use it for illegal purposes.

---

[23] Normal duty hours are 6:00 a.m. to 6:00 p.m.

[24] SSA-71 *Application for Leave*; SSA-2042 *Administrative Time & Leave Record*; SSA-170 *Employee Suggestion Form*.

[25] The legitimate requirement of a person or organization to know, access, or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission.

Conclusions and Recommendations

SSA's extensive use of employee SSNs in its systems and documents increases the risk that the employee SSN may be accessed by unauthorized personnel. SSA has mitigated this through some safeguards, but additional actions are needed. With the increasing impact of identity theft on the public and economy, and as the initiator of SSNs, SSA should become the model for both the public and private sectors by taking the leadership role in protecting SSNs, including those of its employees.

We recommend SSA:

1. Remind employees to secure any system or document containing employee SSNs when these systems or documents are not being used.

2. Consider using asterisks, if determined to be cost-effective, to hide the employee SSN on computer screens and reports in all existing and future systems. Asterisks are currently used in the Mainframe Time and Attendance System to hide the employee SSN.

3. Identify the forms that request the employee's SSN. If the SSN is not required, eliminate its use on these forms.

4. Determine if it is cost beneficial to use an alternative primary identifier for its employees, such as the one used in the *On-Line University*, for all future SSA systems. If determined to be cost-beneficial, then implement an alternative primary identifier.

5. Consider and use, as indicated in Agency policy, encryption if feasible and not cost prohibitive.

AGENCY COMMENTS

SSA agreed with our recommendations. Further, the Agency agreed that it needed to exercise due diligence in protecting employee SSNs. The Agency noted that unlike the private sector, it is bound by Executive Order 9397 and the 1961 Civil Service Commission directives, which mandate the use of SSNs as the identifier of Federal employees. As a result, the Agency states that until such time as both directives are rescinded or modified, it is required to use the SSN as the employee identifying number.

Also, in its response to Recommendation 5, the Agency believes it is already in compliance with the intent of our recommendation. The Agency indicates the use of dedicated lines and Connect Direct when transmitting payroll information to the DOI complies with its policy concerning the transmission of sensitive data outside the Agency. The text of SSA's comments is included in Appendix D.

OIG RESPONSE

We agree the Agency is in compliance with its policy concerning the transmission of sensitive data outside the Agency. Additionally, we agree the use of dedicated lines, Connect Direct, or other secure transport mechanism(s) will provide some level of security for the transmitted data. However, we believe the Agency should also encrypt this sensitive data when transmitted outside the Agency. Data encryption would provide an additional level of security.

Appendices

Acronyms

DOI	Department of Interior
FTC	Federal Trade Commission
GAO	Government Accountability Office
HRMIS	Human Resources Management Information System
MTAS	Mainframe Time and Attendance System
OIG	Office of the Inspector General
OPM	Office of Personnel Management
SSA	Social Security Administration
SSN	Social Security Number
U.S.C.	United States Code

Background, Scope and Methodology

Government Accountability Office

The Government Accountability Office, formerly known as the General Accounting Office (GAO), found[1] that in the course of using Social Security numbers (SSN) to administer programs and as employers, Federal agencies sometimes display SSNs on documents, such as eligibility cards or employee badges. As a result, the SSNs can be seen by others who may not have a need to know. GAO also found that, when requesting SSNs, agencies are not consistently providing individuals with information required by Federal law.[2] Although agencies that use SSNs to provide benefits and services are taking steps to safeguard the numbers from improper disclosure, GAO identified potential weaknesses in the security of information systems at all levels of Government.

Office of the Inspector General

In December 2002, the Office of the Inspector General reported,[3] "…although the Social Security Administration (SSA) has controls over the access, disclosure and use of SSNs by external entities, there was concern about the Agency's exposure to improper SSN attainment and misuse." There were several instances in which SSA personnel unnecessarily displayed SSNs on documents sent to external entities that may not have had a need to know. In addition, there were instances in which SSA personnel were not adequately monitoring contractors' access and use of SSNs.

Scope and Methodology

To accomplish our objectives, we:

- Identified and reviewed applicable laws and regulations;
- Identified and reviewed relevant SSA policies and procedures;
- Identified and reviewed prior relevant audits;
- Interviewed SSA personnel responsible for controls over the use of SSNs;
- Identified and reviewed pertinent SSA employee forms that include SSNs;
- Identified and reviewed pertinent SSA employee forms that include unique identifiers other than SSNs;

[1] *Social Security Numbers – Government Benefits from SSN Use but Could Provide Better Safeguards,* GAO-02-352, May 2002.
[2] The Privacy Act of 1974, 5 U.S.C. § 552a.
[3] *Review of Social Security Administration's Controls Over the Access, Disclosure, and Use of Social Security Numbers by External Entities*, (A-08-02-22071), December, 2002. See Appendix C.

- Determined the Agency's internal usage of SSNs; and
- Observed the safeguards implemented by the Agency.

We performed our review at SSA Headquarters in Baltimore, Maryland. The entities reviewed were the Office of Personnel, and Office of Training within the Office of Human Resources; the Office of the Chief Information Officer; the Office of Public Disclosure within the Office of General Counsel; and the Office of Financial Policy and Operations within the Office of Finance, Assessment and Management. We performed our audit from September 2003 through January 2004 in accordance with generally accepted government auditing standards.

Prior Office of the Inspector General Review

Review of Social Security Administration's Controls over the Access, Disclosure, and Use of Social Security Numbers by External Entities (A-08-02-22071), issued December 30, 2002

To view the appendices for this report, please visit our web site at www.socialsecurity.gov/oig/ or click on the following link http://www.socialsecurity.gov/oig/ADOBEPDF/A-08-02-22071.pdf. If you do not have access to the Internet, you may request a copy of the report by contacting the Office of the Inspector General's Public Affairs Specialist at (410) 966-1375.

Agency Comments

SOCIAL SECURITY

MEMORANDUM 33255-24-1142

July 27, 2004 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Acting Inspector General

From: Larry W. Dye /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report "Social Security Administration's Internal Use of the Social Security Number" (A-13-04-24046)--INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report content and recommendations are attached.

Please let me know if you have any questions. Staff inquiries may be directed to Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT "THE SOCIAL SECURITY ADMINISTRATION'S (SSA) INTERNAL USE OF EMPLOYEES' SOCIAL SECURITY NUMBERS (SSN)" (A-13-04-24046)

Thank you for the opportunity to review and comment on the subject report. We appreciate OIG's continuing efforts to identify opportunities to minimize improper disclosure of our employees' SSNs. We agree that we need to exercise due diligence in protecting the SSNs of our employees; however, unlike the private sector, we are bound by the 1943 Executive Order number 9397 and the 1961 Civil Service Commission (now known as the Office of Personnel Management) directives, both of which mandate the use of the SSN as the identifier of Federal employees. Therefore, until such time as both directives are rescinded or modified, we are required to use the SSN as the employee identifying number. From an overall security perspective, we recognize that limiting the display of an employee's SSN is a prudent measure, and will consider doing so as time and resources allow. Our responses to the specific recommendations are provided below:

Recommendation 1

SSA should remind employees to secure any system or document containing employee SSNs when these systems or documents are not being used.

Response

We agree. Our Office of Systems Security Operations Management and the Agency's Chief Security Officer already issue periodic and ad hoc bulletins to SSA employees concerning systems security matters. Generally, the bulletins focus on systems security issues impacting a wide range of users and developers, or are applicable to the entire Agency. We have established systems security policies and procedures that require a suite of controls over systems that contain sensitive data, such as SSA clients' SSNs and SSA employee SSNs. The Information Systems Security Handbook, and Agency policy governing systems development (i.e., the Systems Development Life Cycle) require documentation of security risk, security plans to address those risks, access controls, audit trails, and other controls in the development of SSA systems. Since there are no findings that indicate these policies and procedures are not being followed, we believe the existing processes are effective.

We recognize that the functions described above are not substitutes for staff taking responsibility for the security of the data they manage and the systems they develop, whether programmatic or administrative, and whether the data is handled electronically or by hardcopy. Therefore, we will take steps to ensure managers and staff adhere to the existing procedures and handling of documents associated with administrative activities.

Recommendation 2

SSA should consider using asterisks, if determined to be cost-effective, to hide the employee SSN on computer screens and reports in all existing and future systems. Asterisks are currently used in the Mainframe Time and Attendance System to hide the employee SSN.

Response

We agree that from an overall security perspective, the use of asterisks to mask on-screen SSNs is a prudent protection measure. We will consider the costs and benefits of using asterisks during the development of future systems enhancements.

Recommendation 3

SSA should identify the forms that request the employee's SSN. If the SSN is not required, eliminate its use on these forms.

Response

We agree that from an overall security perspective the elimination of the collection of SSNs on forms where it is not required is a prudent protection measure. As we review and modify internal forms in the future, we will consider the continuing need to capture the SSN.

Recommendation 4

SSA should determine if it is cost beneficial to use an alternative primary identifier for its employees, such as the one used in the *On-Line University* for all future SSA systems. If determined to be cost-beneficial, then implement an alternative primary identifier.

Response

We agree. However, as noted above, we are bound by the Executive Order number 9397 and Civil Service Commission (now known as the Office of Personnel Management) mandate to use the SSN as the identifying number for Federal employees. In the future, on a case-by-case basis, we will assess the feasibility of using an alternative primary identifier such as the one used in the *On-Line-University*.

Recommendation 5

SSA should consider and use, as indicated in Agency policy, encryption if feasible and not cost prohibitive.

Response

We agree. However, we believe we are already in compliance with the intent of the recommendation. Our current policy (published in 2003 - Appendix H of the Systems Security Handbook) states:

> *In all instances where SSA data is transmitted outside of SSA, encryption must be considered and used if feasible and not cost prohibitive.*
>
> *Any sensitive data transmitted outside of SSA's firewall must be encrypted. This is to be accomplished by dedicated lines, use of connect direct or other secure transport mechanism(s). The method of transport used is dependent upon the application, data transmitted and the receiving party.*

Because we currently use dedicated lines and Connect Direct when transmitting payroll information to the Department of Interior (the example cited in the report), we believe that we are in compliance with the policy as written.

In addition to the items listed above, SSA also provided technical comments, which have been addressed, where appropriate, in this report.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Shirley E. Todd, Director, General Management Audit Division, (410) 966-9365

Brian Karpe, Audit Manager, (410) 966-1029

Acknowledgments

In addition to those named above:

Joe Borowy, Auditor-in-Charge

Cheryl Robinson, Writer-Editor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-1375. Refer to Common Identification Number A-13-04-24046.

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.