
**OFFICE OF
THE INSPECTOR GENERAL**

SOCIAL SECURITY ADMINISTRATION

**PRISONERS' ACCESS TO
SOCIAL SECURITY NUMBERS**

August 2006

A-08-06-16082

AUDIT REPORT



Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, 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

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.



SOCIAL SECURITY

MEMORANDUM

Date: August 23, 2006

Refer To:

To: The Commissioner

From: Inspector General

Subject: Prisoners' Access to Social Security Numbers (A-08-06-16082)

OBJECTIVE

Our objective was to assess the extent to which prisoners have access to Social Security numbers (SSNs) through work programs and the potential risks associated with such access.

BACKGROUND

Some prisons allow inmates to work while incarcerated. While performing some job functions, prisoners have access to other individuals' SSNs. In 1999, the Government Accountability Office found that inmates in the Federal Bureau of Prisons (BoP) and State prison systems had access to personal information (including SSNs) through correctional industry work programs. These inmates performed such duties as data entry as well as duplicating and scanning medical records, automobile registrations, and unemployment records for Federal, State, or local governments.¹ Pending Federal legislation, if enacted, would prohibit executive, legislative, and judicial agencies, as well as instrumentalities of the Federal Government or of a State or political subdivision thereof, from employing prisoners in any capacity that allows prisoners access to SSNs.² Furthermore, the BoP prohibits inmates from scanning documents containing sensitive information.³

We contacted the Department of Corrections and correctional industry work programs in all 50 States and the BoP. We asked each State and the BoP whether inmates were allowed access to SSNs through their job duties and whether a State statute or policy

¹ Government Accountability Office report, *Prison Work Programs: Inmates' Access to Personal Information* (GAO/GGD-99-146), August 1999.

² 2005 H.R. 1745, *Social Security Number Privacy and Identity Theft Prevention Act of 2005*, § 105, *Prohibition of Inmate Access to Social Security Account Numbers*, introduced April 2005.

³ BoP Program Statement 1237.11, Section 9.e., *Inmate Use of Computers, Document Scanners*, October 24, 1997.

prohibited such access. We also made site visits to three prisons in which inmates were allowed access to SSNs. Appendix A contains additional details regarding our scope and methodology. Appendix B contains a list of States and the number of prisons in each State that allow inmate access to SSNs.

RESULTS OF REVIEW

Based on our interviews with State Department of Corrections and correctional industry work programs personnel and reviews of prison policies and practices, we are concerned about prisoners' access to SSNs.⁴ Despite the increasing threat of identity theft, we identified prisons in 13 States that allowed inmates access to SSNs through various work programs. Although prisons placed controls over SSN access, vulnerabilities remained. Based on our previous audit and investigative findings, we know that unnecessary access, disclosure, and use of SSNs increases the potential for dishonest individuals to obtain and misuse these numbers, thus creating SSN integrity issues. Some State and prison officials with whom we spoke shared our concern and have taken additional steps to limit prisoners' access to SSNs.

SOME PRISONS ALLOWED INMATES ACCESS TO SSNs THROUGH PRISON WORK PROGRAMS

Of the 50 States we contacted, 13 (26 percent) allowed inmates access to SSNs through prison work programs (see Appendix B). Prisoners had access to SSNs by performing such duties as data processing, optical imaging, scanning, and records conversion of documents for State agencies, universities, hospitals, and private businesses. The types of documents inmates viewed included marriage, birth, and death certificates; vehicle accident reports; tax appeal documents; and medical claims, all of which generally contained personal identifying information (including SSNs). The following examples illustrate how some States allowed prisoners access to SSNs.

- At six correctional facilities in Tennessee, prisoners scanned and entered motor vehicle titles and registration forms, traffic citations, and insurance cancellation claims, which generally contained SSNs.
- At two correctional facilities in Oklahoma, prisoners converted such documents as payroll records, vehicle titles, and medical records into microfilm or optical images. These documents generally contained personal identifying information (including SSNs).
- At one correctional facility in Nebraska, prisoners entered SSNs from wage and medical claims records. For the State's correctional industry purchasing department, inmates filed purchase orders, which contained the purchasers' tax identification numbers or SSNs.

⁴ Our interviews with the Federal BoP revealed that it does not permit inmate access to SSNs. Accordingly, our concern is limited to State correctional facilities that continue to allow such access.

Correctional industry personnel told us States allow prisoners to perform various jobs because it gives them a sense of self-worth, provides them an income, and equips them with skills they can use upon release from prison. In addition, some States generate income from correctional industry work program contracts that allow prisoners access to personal information. Further, the State agencies that contract with the prisons for these services generally save money because prisoners receive lower wages than the general population. Although we recognize these benefits, we question whether prisoners have a need to know other individuals' SSNs. We believe allowing prisoners access to SSNs increases the risk that individuals may improperly obtain and misuse the SSN. In fact, correctional industry officials acknowledged the potential risks for identity theft and fraud, and one State director told us her State is committed to eliminating inmate access to SSNs. She stated our review helped focus attention on the need to better safeguard SSNs.

We believe States can reduce the risk of prisoners improperly obtaining and misusing SSNs by employing them in jobs that do not involve SSN access. For example, we reviewed the National Correctional Industries Association directory and identified numerous jobs, such as metal fabrication, woodworking, sewing, and food processing that do not generally require prisoner access to SSNs. These types of jobs provide prisoners with valuable skills and generate income for States, while limiting SSN access.

PRISONS PLACED CONTROLS OVER INMATE ACCESS TO SSNs BUT VULNERABILITIES STILL EXISTED

Prisons had some controls in place to safeguard SSNs. For example, some prisons (1) monitored inmate activity through security cameras and guards, (2) searched inmates before entering and exiting the worksite, (3) required that inmates sign a confidentiality agreement stating they would not improperly disclose and/or use SSNs, and (4) counted and verified batches of documents before and after completion of work. In addition, some prisons prohibited inmates convicted of identity theft from working in jobs in which they had access to SSNs.

While we recognize prisons have controls to protect SSNs, we are concerned that individuals intent on criminal activity may attempt to circumvent these controls. For example, prisoners interested in improperly obtaining an SSN could memorize an SSN obtained through their job duties and use it to create a false identity. Moreover, we question whether requiring that prisoners sign a confidentiality agreement is an effective control to prevent SSN misuse and ensure SSN integrity.

Although we did not identify instances in which prisoners improperly obtained and misused SSNs at the prisons we visited, we believe the potential for such activity exists. The following example illustrates how inmates can gain access to personal identifying information when prisons do not have adequate controls in place.

- Inmates at a California prison allegedly gained access to personal information about employees, including their SSNs, birth dates and pension account information, while working in a warehouse where the confidential information was stored. The fact that inmates worked in the warehouse violated a law⁵ barring the Department of Corrections from assigning prisoners to jobs that give them access to others' personal information (including SSNs). In fact, one prisoner found with confidential records reportedly asked an inmate serving time for identity theft to teach him how to use the information. Prison officials did not know how many prisoners might have obtained the personal information. The incident is being investigated.

SOME STATES HAD TAKEN STEPS TO LIMIT PRISONER ACCESS TO SSNs

The increase in identity theft and the recognition that SSNs are linked to vast amounts of personal information have led some States to reconsider the practice of allowing prisoners access to SSNs. Some States have taken steps to limit prisoners' access to SSNs or have discontinued jobs that allowed such access. In addition, some States have enacted laws to regulate prisoners' access to SSNs.⁶ The following examples illustrate how three States limit prisoners' access to SSNs.

- A correctional complex in Kentucky used software to redact personal information from documents processed by prisoners. After correctional industry employees scan documents, the redaction software removes personal information before the prisoner receives it for processing. Once prisoners complete data entry duties, the software merges the personal information back onto the document. Throughout the process, prisoners do not have access to the entire SSN.
- A correctional facility in North Carolina instructed prison employees to remove SSNs from order forms before inmates processed them. North Carolina has also stopped allowing prisoners to access SSNs through its work release jobs and inmate work assignments.
- Utah Correctional Industries used software to redact portions of SSNs from health forms that prisoners processed for a State agency. While the redaction process prevented most prisoners from seeing individuals' entire SSNs, a few prisoners scanned the forms before the redaction process, which allowed them to view the entire SSN.

Although officials at Oklahoma Correctional Industries told us they had redaction software, they did not use it because their clients requested them not to do so. Officials told us their clients believed such software increased the cost and time for document preparation, and data were more secure with prisoners because they could not take the

⁵ California Penal Code §§ 4017.1 and 5071.

⁶ These States include California (California Penal Code §§ 4017.1 and 5071), Illinois (§ 730 ILCS 5/3-12-15), and Texas (Tex. Gov't Code § 497.011).

information home with them. Furthermore, clients believed prison security measures, such as security cameras, full-time supervision, and screening of prisoner mail and telephone calls were adequate to prevent improper SSN attainment.

CONCLUSION AND RECOMMENDATIONS

Despite the risks associated with prisoners' access to SSNs, some prisons continue this practice. While we recognize SSA cannot prohibit prisons from allowing prisoners access to SSNs, we believe it can help reduce potential threats to SSN integrity by encouraging States to limit SSN access. We also recognize that some States generate income or save money from correctional industry work program contracts. However, given the potential threats to SSN integrity, we believe SSA should take steps to safeguard SSNs. Accordingly, we recommend that SSA:

1. Coordinate with Department of Corrections and correctional industry work programs to educate them about the potential risks associated with allowing prisoners access to SSNs. For example, we believe SSA should consider hosting or participating in conferences to discuss ways prisons can enhance SSN integrity.
2. Encourage prisons to limit prisoners' access to SSNs. For example, we believe prisons should safeguard SSNs by limiting access to prison personnel with a need to know and avoid displaying the entire SSN on any document, screen, or data collection field.
3. Promote the best practices of prisons that are taking steps to limit prisoners' access to SSNs. For example, SSA could contribute articles to Department of Corrections/correctional industries journals and association newsletters.

AGENCY COMMENTS

SSA agreed with our recommendations. The Agency's comments are included in Appendix C.



Patrick P. O'Carroll, Jr.

Appendices

[APPENDIX A](#) – Scope and Methodology

[APPENDIX B](#) – States That Allow Prisoners Access to Social Security Numbers

[APPENDIX C](#) – Agency Comments

[APPENDIX D](#) – OIG Contacts and Staff Acknowledgments

Scope and Methodology

To accomplish our objectives, we

- reviewed applicable laws and regulations;
- reviewed a prior Government Accountability Office report;
- contacted 50 States and the Federal Bureau of Prisons to determine whether prisoners were allowed access to Social Security numbers; and
- visited three prisons in two States that allowed prisoners access to Social Security numbers.

The entity audited was the Social Security Administration's Office of the Deputy Commissioner for Operations. Our review of internal controls was limited to information provided by the State departments of corrections and the State correctional industries' work programs for the 50 States and the Federal Bureau of Prisons. We conducted our audit from October 2005 through April 2006 in accordance with generally accepted government auditing standards.

States That Allow Prisoners Access to Social Security Numbers

	State	Number of Facilities Allowing Access	Work Program and Type of Work
1	Alabama	1	Correctional Industry (CI) – data entry
2	Arkansas	1	CI – digital imaging
3	Connecticut	1	CI – data processing
4	Kansas	5	Work Release – data entry and counseling; CI – data entry and microfilm; Internal to Prison – data entry and counseling
5	Montana	1	Internal to Prison – data entry
6	Nebraska	1	CI – data entry; Internal to Prison – filing
7	New Mexico	1	CI – microfilm
8	North Carolina	1	CI – processing order forms
9	Oklahoma	2	CI – records conversion, microfilm, and optical imaging
10	South Dakota	1	CI – data entry
11	Tennessee	6	Work Release – different duties at different businesses; CI – imaging/scanning, data entry, field telephone calls, cleaning test materials
12	Utah	1	CI – data entry and scanning
13	West Virginia	Unknown*	Work Release – type of service depends on the business

***West Virginia stated that inmates may have access to Social Security numbers through employment in work release programs. Specific correctional facilities were not named.**

Agency Comments



SOCIAL SECURITY

MEMORANDUM

Date: August 11, 2006 **Refer To:** S1J-3

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

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

Subject: Office of the Inspector General (OIG) Draft Report, "Prisoners' Access to Social Security Numbers" (A-08-06-16082)—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 we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF INSPECTOR GENERAL (OIG) DRAFT REPORT, “PRISONERS’ ACCESS TO SOCIAL SECURITY NUMBERS” (A-08-06-16082)

Thank you for the opportunity to review and comment on the draft report. We appreciate your conducting this audit of prisoners’ access to Social Security numbers (SSN). The Agency has taken steps and has planned actions to reduce the potential risk associated with allowing prisoners access to SSNs.

Recommendation 1

SSA should coordinate with the Department of Corrections and with the correctional industry work programs to educate them about the potential risks associated with allowing prisoners access to SSNs. For example, OIG believes that SSA should consider hosting or participating in conferences to discuss ways prisons can enhance SSN integrity.

Comment

We agree and support outreach efforts to educate the correctional community. As you know, the Commissioner and SSA’s Inspector General, under joint signature, just recently wrote to the National Correctional Industries Association, the National Sheriff’s Association, the American Correctional Association, and the American Jail Association, to inform them of the potential risks associated with prisoner access to SSNs. In addition, the Agency continues to disseminate information on this subject by coordinating educational outreach programs and public information programs with correctional officials on a local, regional and national basis, and by having our public information specialists conduct workshops and seminars with prison officials regarding the potential risks.

Recommendation 2

SSA should encourage prisons to limit prisoners’ access to SSNs. For example, OIG believes prisons should safeguard SSNs by limiting access to prison personnel with a need to know and avoid displaying the entire SSN on any document, screen, or data collection field.

Comment

We agree. However, we believe that prison officials should safeguard SSNs by not allowing prisoners access to *any* documents, screens, or data collection fields that display an SSN. The Agency believes encouraging prisons to limit prisoners’ access to SSNs will prevent potential fraudulent use of SSNs by prisoners. As detailed in the recent letters (referenced above in our reply to Recommendation 1), alternatives exist and the Agency

believes that prisons should either investigate the redaction software used by correctional industry work programs that prevent access to entire SSNs or reassign prisoners to jobs that do not require access to SSNs.

Recommendation 3

SSA should promote the best practices of prisons that are taking steps to limit prisoners' access to SSNs. For example, SSA could contribute articles to the Department of Corrections/correctional industries journals and association newsletters.

Comment

We agree. The Agency supports public information and public education programs with correctional officials that promote best practices of those prisons that help safeguard the integrity of the SSN by preventing prisoner access. Some of these best practices were detailed in the letters recently sent to the prison associations referenced above in our reply to Recommendation 1.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kimberly A. Byrd, Director, 205-801-1605

Jeff Pounds, Audit Manager, 205-801-1606

Acknowledgments

In addition to those named above:

Janet Matlock, Auditor in Charge

Theresa Roberts, Audit Manager

Kimberly Beauchamp, 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) 965-3218. Refer to Common Identification Number A-08-06-16082.

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 Resource Management (ORM). 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 Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM 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.