OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

UNIVERSITIES' USE OF SOCIAL SECURITY NUMBERS AS STUDENT IDENTIFIERS IN REGION VIII

March 2005 **A-04-05-15039**

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.

SOCIAL SECURITY

MEMORANDUM

Date: March 21, 2005 Refer To:

To: James C. Everett
Regional Commissioner
Denver

From: Inspector General

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region VIII (A-04-05-15039)

OBJECTIVE

Our objective was to assess universities' use of Social Security numbers (SSN) as student identifiers and the potential risks associated with such use.

BACKGROUND

Millions of students enroll in educational institutions each year. To assist in this process, many colleges and universities use students' SSNs as personal identifiers. The American Association of Collegiate Registrars and Admissions Officers found that half of member institutions that responded to a 2002 survey used SSNs as the primary student identifier.[1] Although no single Federal law regulates overall use and disclosure of SSNs by colleges and universities, the Privacy Act of 1974, the Family Educational Rights and Privacy Act, and the Social Security Act contain provisions that govern the disclosure and use of SSNs. See Appendix A for more information on the specific provisions of these laws.

POTENTIAL RISKS ASSOCIATED WITH COLLECTING AND USING SSNs

While the schools we selected did not report any instances of identity theft or fraud, many universities' collection and use of SSNs entail certain risks. Each time an individual divulges his or her SSN, the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases. We believe the following examples illustrate students'

[1] *Academic Transcripts and Records: Survey of Current Practices,* April 2002 Special Report, the American Association of Collegiate Registrars and Admissions Officers.

risk of exposure to such activity. Because many universities still use SSNs as the primary identifier, students' exposure to identity theft and fraud remains today.

- A university professor in Washington was indicted on 33 counts of mail fraud in a scam using students' SSNs. The professor allegedly accessed the university's records system and used students' information to obtain new SSN cards by posing as a parent. The professor then allegedly used the SSNs to obtain credit cards and birth certificates.

- California authorities arrested a man suspected of stealing the names and SSNs of 150 college students and using that information to obtain credit cards and charge more than $200,000 in the students' names.

- A student at a Texas university was accused of hacking into the school's computer network and downloading the names and SSNs of more than 55,000 students, faculty, and alumni.

- A gentleman discovered a computer printout in a trash bin near a Pennsylvania university listing SSNs and other personal data for hundreds of students.

SCOPE AND METHODOLOGY

We selected a sample of 12 educational institutions in Region VIII.[2] For each selected school, we interviewed university personnel and reviewed school policies and practices for using SSNs. See Appendices B and C for additional details regarding the scope and methodology of our review and a list of the universities we contacted, respectively.

RESULTS OF REVIEW

Based on our interviews with university personnel and reviews of school policies and practices, we are concerned about universities' use of SSNs as student identifiers. We identified several instances in which universities used SSNs as the primary student identifier or for other purposes, even when another identifier would suffice. However, we are encouraged that officials from many of the universities we contacted shared our concern and stated that their universities had taken, or were planning to take, steps to reduce SSN use as the primary student identifier.

[2] Region VIII consists of the following six States: Colorado, Montana, North Dakota, South Dakota, Utah and Wyoming.

COLLEGES AND UNIVERSITIES CONTINUE TO USE THE SSN AS AN IDENTIFIER

Despite the increasing threat of identity theft, some colleges and universities continue to use the SSN for several purposes, particularly as the primary student identifier. Our visits to 6 colleges and universities and telephone interviews with 6 others revealed that the SSN was used as the student identifier by 6 of the 12 universities we contacted in Region VIII. The following table identifies some uses of the SSN at the universities and colleges contacted and our related concerns.

SSN Use and Related Concerns

SSN USE	CONCERN
Class Registration: At several institutions, students must disclose their SSNs to register for courses (on-line or paper form registration processes).	The paper registration process unduly discloses the SSN to university/college registrar employees throughout the process. The on-line registration process generally results in electronic databases that identify students by SSN. Without strict application controls, individuals' SSNs could be compromised.
Class Rosters: Class rosters at some universities and colleges listed the students' SSNs and names.	Listing SSNs on class rosters with students' names exposes the SSN to university employees. At a minimum, the practice makes SSNs available to instructors. If instructors do not adequately safeguard class rosters, students' names and SSNs could be vulnerable to unauthorized access.
Computer Login: Students must enter their SSNs to log into computers at several of the colleges and universities.	Students' SSNs are susceptible to unauthorized disclosure during the log-in process. At one university/college, the SSN was displayed on the computer monitor during the log-in process. Computer users accustomed to the process could visually obtain an SSN when a student logs on.
Class Grade Reports: Instructors at some of the universities and colleges reported final grades to the registrar's office by students' SSNs.	Listing SSNs and students' names on class grade reports discloses the SSN to university/college employees. This weakens institutional control over the SSN.
Overdue Library Book Reports: At one university/college, library staff maintained overdue library book records that identified the delinquent student by name and SSN.	The paper record of overdue books containing student names and SSNs increases SSN exposure to library staff and other individuals in the work area. Additionally, the electronic database used to develop the overdue book record contained the students SSNs. Without strict application controls the SSN could be electronically compromised.

The institutions that continued to employ the SSN as a primary student identifier recognized the risks associated with this practice and had adopted plans to issue a non-SSN student identifier by the fall 2006 semester. This change will eliminate universities' and colleges' use of the SSN as a student identifier.

Some universities and colleges in Region VIII had already initiated actions to phase out the SSN as a primary student identifier. For example, one university recently redesigned its student information system with the capability to assign and use non-SSN student identification numbers. With the redesigned system, the university began issuing randomly generated student identification numbers to all new students registering for the fall 2003 semester. Students enrolled before fall 2003 will be issued a non-SSN student identifier system starting with the spring 2006 semester. The Registrar stated that, although considerable costs were being incurred in transitioning to non-SSN student identification numbers, university officials fully supported the change, as they recognized the importance of protecting students' personal identities. Additionally, the Registrar stated the university was trying to increase awareness regarding the need to protect the SSN along with other sensitive, personally identifiable information.

All of the colleges and universities we contacted recognized the importance of protecting students' identities along with restricting the use of the SSN as a student identifier. However, officials at several of these institutions cited funding limitations as a hurdle in implementing changes to information systems that would enable the transition to non-SSN student identification numbers. According to these officials, costly enhancements to existing information systems or the implementation of a new student information system is often necessary to support the replacement of the SSN as the primary student identifier. Although funding issues were identified as a roadblock to transitioning away from using the SSN as an identifier, institutions using the SSN as a primary identifier are now prepared to incur the costs and accept the challenges associated with assigning and managing non-SSN student identification numbers.

We did not identify instances in which students' SSNs were misused at the colleges and universities interviewed. However, we believe the potential for misuse is greater at those universities that continue to use the SSN as the primary student identifier. We are encouraged that colleges and universities using the SSN as the primary student identifier have adopted plans to eliminate this practice and will only use it for financial aid and tax purposes. The institutions we contacted acknowledged the risks of using the SSN and will strive to limit SSN exposure.

CONCLUSION AND RECOMMENDATIONS

Despite the potential risks associated with using SSNs as primary student identifiers, some colleges and universities in Region VIII continued this practice. While we recognize SSA cannot prohibit colleges and universities from using SSNs as student identifiers, we believe SSA can help reduce potential threats to SSN integrity by encouraging schools to limit SSN collection and use. We also recognize the challenge of educating such a large number of educational institutions. However, given the potential threats to SSN integrity, such a challenge should not discourage SSA from taking steps to safeguard SSNs. Accordingly, we recommend that SSA:

1. Coordinate with colleges/universities and State/regional educational associations to educate the university community about the potential risks associated with using SSNs as student identifiers.

2. Encourage colleges and universities to limit their collection and use of SSNs.

3. Promote the best practices of educational institutions that no longer use SSNs as student identifiers.

AGENCY COMMENTS

SSA agreed with our recommendations. We believe SSA's response and planned actions adequately address our recommendations and will help strengthen SSN integrity. The full text of SSA's comments is included in Appendix D.

Patrick P. O'Carroll, Jr.

Appendices

Federal Laws that Govern Disclosure and Use of the Social Security Number

The following Federal laws establish a general framework for disclosing and using the Social Security number (SSN).

The Privacy Act of 1974 (5 U.S.C. § 552a; Pub. L. No. 93-579, §§ 7(a) and 7(b))

The *Privacy Act of 1974* provides that it is unlawful for a State government agency to deny any person a right, benefit, or privilege provided by law based on the individual's refusal to disclose his/her SSN, unless such disclosure was required to verify the individual's identity under a statute or regulation in effect before January 1, 1975. Further, under *Section 7(b),* a State agency requesting that an individual disclose his/her SSN must inform the individual whether the disclosure is voluntary or mandatory, by what statutory or other authority the SSN is solicited, and what uses will be made of the SSN.

The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99)

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. FERPA applies to those schools that receive funds under an applicable program of the U.S. Department of Education. Under FERPA, an educational institution must have written permission from the parent or eligible student to release any personally identifiable information (which includes SSNs) from a student's education record.[1] FERPA does, however, provide certain exceptions in which a school is allowed to disclose records without consent. These exceptions include disclosure without consent to university personnel internally who have a legitimate educational interest in the information, to officials of institutions where the student is seeking to enroll/transfer, to parties to whom the student is applying for financial aid, to the parent of a dependent student, to appropriate parties in compliance with a judicial order or lawfully issued subpoena, or to health care providers in the event of a health or safety emergency.

[1] FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the child when the child reaches the age of 18 or attends an institution of postsecondary education. Children that have been transferred rights are referred to as "eligible students."

The Social Security Act

The Social Security Act provides that “Social Security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and that no authorized person shall disclose any such Social Security account number or related record.” (42 U.S.C. §405(c)(2)(C)(viii)). The Social Security Act also provides that “[w]hoever discloses, uses, or compels the disclosure of the Social Security number of any person in violation of the laws of the United States; shall be guilty of a felony…” (42 U.S.C. §408(a)(8)).

Scope and Methodology

To accomplish our objective, we

- interviewed selected university personnel responsible for student admissions/registrations;
- reviewed Internet websites of the 12 colleges and universities we contacted;
- reviewed applicable laws and regulations; and
- reviewed selected studies, articles and reports regarding universities' use of Social Security numbers (SSN) as student identifiers.

We visited six educational institutions and interviewed personnel at six others to learn more about their policies and practices for using SSNs as student identifiers. Our review of internal controls was limited to gaining an understanding of universities' policies over the collection, protection and use/disclosure of SSNs. The Social Security Administration entity reviewed was the Office of the Deputy Commissioner for Operations. We conducted our audit from June through September 2004 in accordance with generally accepted government auditing standards.

Educational Institutions Contacted

We interviewed personnel at 12 educational institutions in Region VIII. The following table shows the names and locations of these schools as well as their total student enrollments.

	School	Location	Student Enrollment
1	Augustana College	Sioux Falls, South Dakota	1,812
2	College of Eastern Utah	Price, Utah	1,924
3	Dawson Community College	Glendive, Montana	389
4	Jamestown College	Jamestown, North Dakota	1,137
5	Laramie County Community College	Cheyenne, Wyoming	2,800
6	South Dakota State University	Brookings, South Dakota	9,690
7	University of Colorado, Boulder	Boulder, Colorado	30,767
8	University of Denver	Denver, Colorado	8,295
9	University of Montana, Missoula	Missoula, Montana	13,032
10	University of North Dakota	Grand Forks, North Dakota	12,605
11	University of Wyoming	Laramie, Wyoming	12,231
12	Utah State University	Logan, Utah	16,318

Source: We determined student enrollment by reviewing university websites or one of the following websites: www.collegeboard.com/splash or www.uscollegesearch.org.

Agency Comments

Wednesday, March 02, 2005

Thank you for the opportunity to review the draft OIG report on the use of Social Security Numbers (SSN) as student identifiers by universities. This report was well written and provided valuable information to us.

We agree with all three recommendations made regarding the need for outreach to the universities and colleges to promote limiting the use of the SSN. Some of our managers are already working with their local colleges to establish a new procedure. Recommendations 1 and 2 could be considered one step – working with the local contacts to understand the risks associated with using the SSN and encourage them to limit the collection and use of SSNs.

We believe these recommendations are worthwhile. We consider this an ongoing project as contacts are made with the colleges by our managers or Public Affairs Specialists. Also, we encourage these recommendations be made at a national level, as this is a national problem. Several of these actions can be implemented nationally to benefit everyone.

If your staff has any questions regarding these comments, they can contact Debbie Sweeney, RSI Programs Branch, at (303) 844-5719.

James C. Everett
Regional Commissioner
Denver

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

Frank Nagy, Deputy Director, (404) 562-5552

Acknowledgments

In addition to those named above:

Phillip Krieger, Auditor-in-Charge

Kimberly Beauchamp, Writer/Editor

For additional copies of this report, please visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-04-05-15039.

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.