

---

**OFFICE OF  
THE INSPECTOR GENERAL**

---

**SOCIAL SECURITY ADMINISTRATION**

---

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

**March 2005**

**A-08-05-15033**

---

**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 8, 2005

Refer To:

To: Carl L. Rabun  
Regional Commissioner  
Seattle

From: Inspector General

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region X  
(A-08-05-15033)

## 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.<sup>1</sup> 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 disclosure and use of SSNs. See Appendix A for more information on the specific provisions of these laws.

We selected a sample of eight educational institutions in Region X.<sup>2</sup> For each selected school, we interviewed university personnel and reviewed school policies and practices for using SSNs. In addition, we identified two schools outside of Region X that no longer used SSNs as student identifiers and determined reasons for this change and best practices that could be adopted by other schools. 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.

---

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

<sup>2</sup> Region X consists of the following four states: Washington, Oregon, Idaho, and Alaska.

## **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. We identified instances in which universities used SSNs as the primary student identifier or for other purposes, even when another identifier would suffice. Based on our previous audit and investigative findings, we know that unnecessary use of SSNs increases the potential for unscrupulous individuals to illegitimately gain access to these numbers and misuse them, thus creating SSN integrity issues. Some university personnel with whom we spoke shared our concern and have taken steps to reduce SSN use.

### **UNIVERSITIES' USE OF SSNs**

Despite the increasing threat of identity theft, some colleges and universities continue to use SSNs for various purposes. Our visits to four colleges and universities and telephone interviews with four others in Region X disclosed that universities used SSNs as the primary student identifier and for admissions applications, class registration, access to computer systems, class rosters, and grade reports.

In Region X, one university official told us her university requests SSNs during admissions and uses them as the primary student identification number. She also told us the State University System requests students' SSNs so it can track student movement and educational outcomes through the K-12 and higher education systems. An official at another university told us her school uses SSNs because they are unique identifiers and are helpful when comparing student transcripts and name changes. The university official also stated her school allows students to use another identification number, although students must formally request to do so.

Another university official told us his Information Technology department uses SSNs to confirm students' identities and ensure the school has correct student records. Also, an official at another university told us her school primarily uses SSNs to retrieve information when student identification numbers are not readily available and to differentiate between student records with the same name.

### **POTENTIAL RISKS ASSOCIATED WITH COLLECTING AND USING SSNs**

While the schools we contacted in Region X did not report any instances of identity theft or fraud, 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. Because many universities still use SSNs as the primary student identifier, students' exposure to identity theft and fraud remains today. We believe the following examples illustrate students' risk of exposure to such activity nationwide and in Region X.

- 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 over \$200,000 in the students' names.
- A New York school notified about 1,800 students that their SSNs and other personal information had been posted on a university website. The university shut down the website and apologized to the students in an e-mail.
- A student at a Texas university was accused of hacking into the school's computer network and downloading the names and SSNs of over 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.

### **SOME UNIVERSITIES AND STATES HAVE TAKEN STEPS TO LIMIT SSN USE**

Numerous incidences of identity theft at colleges and universities and the recognition that SSNs are linked to vast amounts of personal information have led some schools to reconsider the practice of using SSNs as primary student identifiers. Several schools have taken steps to reduce their reliance on SSNs or have turned to alternative identifiers. In addition, some States have enacted laws to regulate college and university use of SSNs.

University personnel we contacted in Region X acknowledged the potential risks for identity theft and fraud, and some have taken steps to reduce their reliance on SSNs. The Registrar at Idaho State University told us her school does not use SSNs as the primary student identifier. Instead, it uses a six-digit identification number to track students within the university system. Also, the Assistant Registrar at Seattle University told us her university issues student identification numbers and has not used SSNs as the primary student identifier since 1997. In addition, the Registrar at the University of Washington told us his university has never used SSNs as the primary student identifier and no longer displays them on student records. Further, the State of Washington requires that institutions of higher education use personal identifiers that are not SSNs.<sup>3</sup>

In addition, we identified two schools outside of Region X that no longer used SSNs as student identifiers and determined reasons for this change and best practices that could be adopted by other schools. In 2003, the Georgia Institute of Technology (Georgia Tech) stopped using SSNs of students, faculty, and staff on identification cards and as

---

<sup>3</sup> Rev. Code Wash. (ARCW) § 28B.10.042.

the primary means of identification in campus databases because of increased identity theft concerns. To replace SSNs, Georgia Tech created the Georgia Tech Identification Number, a unique number the school uses to identify students in most major campus databases. The Associate Registrar told us the conversion from using SSNs as the primary student identifier took about 2 years of planning but was not difficult. In fact, she stated the actual conversion took only 1 weekend. Georgia Tech has provided information to other schools to assist them in their SSN conversion efforts. Georgia Tech collects SSNs for certain services, for example, payroll, immigration and financial aid.

In 2003, the University of Florida replaced the SSN as a student identifier and key to student records with an eight-digit public identification number to reduce the visibility of the SSN during normal university business. The University of Florida changed to an eight-digit number so students would not confuse it with their SSN. Students also have a Gatorlink username and password for on-line class registration and other applications. According to the University Registrar, the conversion from SSNs to an eight-digit student identifier was challenging as it affected every administrative system. He told us it took the university 1-2 years of planning before the conversion. The Registrar also told us that faculty members no longer have access to students' SSNs. While some university offices (admissions, registrar, student financial affairs and university financial services) still need SSNs to perform their duties, faculty and staff do not ask for SSNs, and students are informed that University personnel should not ask for their SSN. The University Registrar told us the University of Florida offices will not collect or use SSNs unless they are needed for State and federally mandated requirements.

Other colleges and universities have taken steps to limit SSN use. Arizona State University, the University of Michigan, Penn State University, the University of Maryland, the University of Illinois, and the University of Texas have specific policies regarding SSN disclosure and use and have stopped using SSNs as the primary student identification number. In addition, several States, including Arizona, New York, Maryland, Rhode Island, and Wisconsin have enacted laws to regulate college and university SSN use.

## **CONCLUSION AND RECOMMENDATIONS**

Despite the potential risks associated with using SSNs as primary student identifiers, many colleges and universities continue this practice. While we recognize that 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.
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 AND OIG RESPONSE**

SSA agreed with our recommendations. We believe SSA's response and planned actions adequately address our recommendations and will help strengthen SSN integrity. SSA also provided technical comments that we considered and incorporated, where appropriate. SSA's comments are included in Appendix D.



Patrick P. O'Carroll, Jr.

# Appendices

---

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

APPENDIX B – Scope and Methodology

APPENDIX C – Educational Institutions Contacted

APPENDIX D – Agency Comments

APPENDIX E – OIG Contacts and Staff Acknowledgments



# 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, note; 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.<sup>1</sup> 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.

---

<sup>1</sup> 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 eight colleges and universities that we either visited or interviewed by telephone;
- reviewed applicable laws and regulations; and
- reviewed selected studies, articles and reports regarding universities' use of Social Security numbers as student identifiers.

We visited four educational institutions and interviewed personnel at four others to learn more about their policies and practices for using Social Security numbers as student identifiers. In addition, we identified two schools that no longer used Social Security numbers as student identifiers and determined reasons for this change and best practices that could be adopted by other schools. 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 October 2004 in accordance with generally accepted government auditing standards.

## Educational Institutions Contacted

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

	<b>School</b>	<b>Location</b>	<b>Student Enrollment</b>
1	University of Washington	Seattle, Washington	48,000
2	Portland State University	Portland, Oregon	22,409
3	Idaho State University	Pocatello, Idaho	13,666
4	University of Alaska – Anchorage	Anchorage, Alaska	13,664
5	Seattle University	Seattle, Washington	3,765
6	Lewis-Clark State College	Lewiston, Idaho	3,471
7	Pacific Northwest College of Art	Portland, Oregon	2,800
8	Alaska Pacific University	Anchorage, Alaska	673

Source: We determined student enrollment by reviewing university websites.

## Agency Comments

Thank you for the opportunity to comment on the draft OIG audit of Universities' Use of Social Security Numbers (SSNs) as Student Identifiers in Region X. We have a few general comments about the draft, as well as responses to the OIG recommendations.

### **Recommendations**

***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.***

We agree with this recommendation. As we continue our regular and ongoing public affairs outreach, we will stress to the institutions and educational associations in the Region the potential risks associated with using SSNs as student identifiers.

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

We agree with this recommendation. As we continue our regular and ongoing public affairs outreach, we will discourage the collection and use of the SSN by colleges and universities.

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

We agree with this recommendation. As we continue our regular and ongoing public affairs outreach, we will cite the examples given in this audit to the institutions and associations contacted. However, it would be helpful if OIG can provide more detail on the experiences of the universities noted on page 5 of the audit, including any available contact information. Any Seattle Region university wishing to follow the lead of one of the institutions cited as moving away from a reliance on SSNs will likely want to discuss details with that university.

If your staff have any questions, they may contact Tim Beard, RSI Programs and Systems Team, at 206 615-2125, or by email at [Tim.Beard@ssa.gov](mailto:Tim.Beard@ssa.gov).

Carl L. Rabun

## **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:

Neha Smith, Auditor-in-Charge

Kathy Youngblood, Senior Auditor

Susan Phillips, Auditor

Kimberly Beauchamp, Writer-Editor

For additional copies of this report, please visit our web site at [www.ssa.gov/oig](http://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-08-05-15033.

## **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.