

---

**OFFICE OF  
THE INSPECTOR GENERAL**

---

**SOCIAL SECURITY ADMINISTRATION**

---

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

**August 2005**

**A-01-05-15071**

---

**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: August 12, 2005

Refer To:

To: Manuel J. Vaz  
Regional Commissioner  
Boston

From: Inspector General

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region I  
(A-01-05-15071)

## 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 B for more information on the specific provisions of these laws.)

## SCOPE AND METHODOLOGY

We selected a sample of 12 educational institutions in Region I.<sup>2</sup> For each selected school, we contacted university personnel and reviewed school policies and practices for using SSNs. See Appendices C and D for additional details on the scope and methodology of our review and a list of the educational institutions we contacted,

---

<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 I consists of the following six States: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont.

respectively. We are conducting a review in each of the Social Security Administration's (SSA) 10 regions and will issue separate reports to each Regional Commissioner.

## **RESULTS OF REVIEW**

Based on our contacts 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.

Specifically, for the 12 schools contacted in Region I, we found that:

- 7 used the SSN as the primary identifier and the schools did not provide students with documentation explaining how their SSNs are used,
- 3 did not use the SSN as the primary identifier, and
- 2 had not responded despite numerous follow-up contacts from us.<sup>3</sup>

Of the 7 schools who used the SSN as the primary identifier, we found that:

- 4 had students using their SSNs to register for classes online or by telephone and a fifth school discontinued this practice in May 2005.
- 4 gave instructors access to students' SSNs.
- 4 planned to reduce the use of SSNs as the student identifier, but 3 schools did not have such plans. For example, one university did not have immediate plans to reduce use of the SSN because of other priorities and the high cost involved.

(Schools may fall into one or more of the three categories above.)

## **COLLEGES AND UNIVERSITIES CONTINUED TO USE THE SSN AS AN IDENTIFIER**

Despite the increasing threat of identity theft, some colleges and universities continued to use the SSN for several purposes, particularly as the primary student identifier. The following table identifies some uses of the SSN at the seven universities and colleges who use it as the primary identifier and our related concerns.

---

<sup>3</sup> We initially requested information in February and March 2005 and we followed up several times, but as of July 13, 2005, the schools were not cooperating.

<b>SSN Use and Related Concerns</b>	
<b>SSN USE</b>	<b>CONCERN</b>
<b>Class Registration:</b> At several institutions, students had to disclose their SSNs to register for courses (on-line or by telephone).	The on-line registration process generally results in electronic databases that identify students by SSN. Without strict application controls, individuals' SSNs could be compromised.
<b>Class Rosters:</b> Class rosters at some universities and colleges listed the students' SSNs and names.	Listing SSNs on class rosters with students' names exposes the SSNs 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.
<b>Transcripts:</b> Several institutions provided transcripts to students with their SSNs appearing on the documents.	Transcripts are requested in person or are mailed to the students' addresses. Listing the SSNs on transcripts exposes the SSN if it is stolen through the mail or to anyone who comes in contact with a student's transcript.
<b>Class Grade Reports:</b> 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 SSNs to university/college employees. This weakens institutional control over the SSN.

Some universities and colleges in Region I had initiated actions to phase out the SSN as a primary student identifier. For example, one university will be assigning all students new identification numbers beginning in the summer of 2005. All students (new and current) will receive a randomly generated student identification number and a new identification card by the fall semester of 2005. Additionally, based on our interview, one school is planning to eliminate the SSN from official transcripts issued to students and third parties.

Most 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. Additionally, the Registrar for one institution stated the college did not intend to change its use of the SSN as a student identifier because it is easier to track and identify students by their SSNs. However, all of the colleges and

universities we contacted that used the SSN as a student identifier, stated that students have the option of using another number as an identification number.

We did not identify instances in which students' SSNs were misused at the colleges and universities included in our audit. 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 some of the 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.

## **LEGISLATION RELATED TO SSN USE AND IDENTITY FRAUD**

During Calendar Year 2004, two of the six States in Region I passed legislation on the use or display of the SSN, and one State passed legislation related to identity fraud.

- Connecticut passed legislation that prohibits an entity that purchases a housing project from disclosing to the public the tenants' SSNs from the tenants' lease agreements. Additionally, this legislation prohibits housing authorities from disclosing the SSNs of tenants to anyone except a purchaser of a housing project without the tenant's permission.<sup>4</sup>
- New Hampshire passed legislation that increased the penalty for identity fraud.<sup>5</sup>
- Vermont passed legislation that makes it a crime to obtain, produce, possess, use, sell, give, or transfer personal identifying information (including SSNs) belonging or pertaining to another person with intent to use the information to commit a misdemeanor or a felony.<sup>6</sup> Additionally, this legislation requires that a study be completed related to the use of SSNs by both public and private entities and that proposals be developed to reduce such use wherever possible and protect privacy and security when the numbers must be used.<sup>7</sup>

---

<sup>4</sup> Connecticut General Statutes § 8-64b.

<sup>5</sup> Revised Statutes Annotated 638:26.

<sup>6</sup> Thirteen Vermont Statutes Annotated § 2030, §§ 4-5.

<sup>7</sup> The *Identity Theft Study Committee Report On the Use of Social Security Numbers* was issued to the State Legislature in January 2005 and it recommends that legislation be proposed that would restrict the use of SSNs. Specifically the report recommended that this legislation implement the following restrictions on the use of SSNs: (1) no public posting or display of an individual's SSN; (2) no printing of an SSN on any card required to access products or services; (3) prohibition against any requirement of the transmission of an SSN over the Internet, unless secure connection or SSN is encrypted; (4) prohibition against any requirement of an SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required for access; and (5) prohibition against any use of SSNs on any materials that are mailed (certain exceptions apply).

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

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

- A computer at Boston College that contained the SSNs of about 100,000 alumni was breached by a hacker in March 2005. As a result of this breach, Boston College took immediate action to purge all SSNs from this system and from all alumni records.
- Tufts University—a school in Medford, Massachusetts—sent letters to 106,000 alumni in April 2005 warning of abnormal activity on a computer that contained names, addresses, telephone numbers, and in some cases, Social Security and credit card numbers.
- A former Tufts University medical student was arrested and sentenced to 364 days in Federal prison in April 2005 after pleading guilty to fraudulently obtaining more than \$150,000 in loans and scholarships by using false identities and SSNs to secure the funds and admission to other schools, after his student visa expired.

## **CONCLUSION AND RECOMMENDATIONS**

Despite the potential risks associated with using SSNs as primary student identifiers, some colleges and universities in Region I 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, as resources permit:

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. Specifically, SSA field office staff will discuss with the institutional officials the risks associated with using SSNs as student identifiers, encourage officials to limit the collection and use of SSNs, and share best practices of those institutions that no longer use SSNs as student identifiers. (See Appendix E for the Agency's comments.)

A handwritten signature in black ink, appearing to read "Patrick P. O'Carroll, Jr.", with a stylized flourish at the end.

Patrick P. O'Carroll, Jr.



# Appendices

---

[APPENDIX A](#) – Acronyms

[APPENDIX B](#) – Federal Laws that Govern Disclosure and Use of the Social Security Number

[APPENDIX C](#) – Scope and Methodology

[APPENDIX D](#) – Educational Institutions Reviewed

[APPENDIX E](#) – Agency Comments

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

## Acronyms

C.F.R.	Code of Federal Regulations
FERPA	Federal Educational Rights and Privacy Act
SSA	Social Security Administration
SSN	Social Security Number
U.S.C.	United States Code

## 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; Public Law 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 who have been transferred these rights are referred to as "eligible students."

### *The Social Security Act*

The Social Security Act provides that “[s]ocial 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 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, or information systems;
- 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 contacted 12 universities and colleges in the New England area. Of those 12, we visited 6 and contacted personnel at 6 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 February through May 2005 in accordance with generally accepted government auditing standards.

## Educational Institutions Reviewed

The following table shows the names, locations, and total undergraduate student enrollments for the 12 educational institutions contacted in Region I.

	<b>School</b>	<b>Location</b>	<b>Student Enrollment</b>
1	Charter Oak State College	New Britain, Connecticut	1,495
2	University of Hartford	West Hartford, Connecticut	5,300
3	University of Maine	Orono, Maine	8,397
4	St. Joseph's College	Standish, Maine	960
5	Northeastern University	Boston, Massachusetts	14,618
6	Clark University	Worcester, Massachusetts	2,082
7	University of New Hampshire	Durham, New Hampshire	10,942
8	Rivier College	Nashua, New Hampshire	1,447
9	University of Rhode Island	Kingston, Rhode Island	10,957
10	Rhode Island College	Providence, Rhode Island	6,771
11	Champlain College	Burlington, Vermont	2,307
12	University of Vermont	Burlington, Vermont	8,156

Source: We determined student enrollment by reviewing the following website: [www.collegeboard.com](http://www.collegeboard.com).

## Agency Comments



## SOCIAL SECURITY

### MEMORANDUM

**Date:** July 28, 2005

**Refer To:** S2D1G3/ER

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

**From:** Manuel J. Vaz  
Regional Commissioner  
Boston

**Subject:** Universities' Use of Social Security Numbers as Student Identifiers in Region I  
(A-01-05-15071)

Thank you for the opportunity to comment on the draft audit report on Universities' use of the SSN as student identifiers in our Region. Our comments on each of the three recommendations are provided below.

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.

Most of our field offices parallel to colleges and universities have an ongoing relationship with the institutional officials for various reasons such as enumeration and recruitment. During these contacts, we will discuss with the institutional officials the risks associated with using SSNs as student identifiers.

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

During the contacts mentioned in response to the first recommendation, we will encourage officials to limit their collection and use of the SSNs. We agree, however, with the comments made by the Acting Regional Commissioner of the Kansas City Region that this recommendation may not be practical to implement. We believe that the use of the SSN is pervasive for many reasons (financial assistance applications being just one).

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

In our contacts with college and university officials, we will include a discussion of the best practices of those institutions that no longer use SSNs as student identifiers.



Again, thank you for the opportunity to comment on this draft. If members of your staff have any questions they may contact Sharon Valerio of the Center for Programs Support at 617-565-2882.

cc: Deputy Director, Office of Audit, Boston

## **OIG Contacts and Staff Acknowledgments**

### ***OIG Contacts***

Judith Oliveira, Director, Boston Audit Division, (617) 565-1765

David Mazzola, Audit Manager, (617) 565-1807

### ***Acknowledgments***

In addition to those named above:

Frank Salamone, Auditor

Melinda Tabicas, Auditor

For additional copies of this report, please visit our web site at [www.socialsecurity.gov/oig](http://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-01-05-15071.

## **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.