OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

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

April 2005 **A-13-05-15083**

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: April 26, 2005 Refer To:

To: Laurie Watkins
Regional Commissioner
Philadelphia

From: Inspector General

Subject: Universities' Use of Social Security Numbers as Student Identifiers in Region III (A-13-05-15083)

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 almost 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 disclosure and use of SSNs. See Appendix A for more information on the specific provisions of these laws.

We selected a sample of 12 universities[2] in Region III.[3] For each selected university, 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.

---

[1] *Academic Transcripts and Records: Survey of Current Practices,* April 2002 Special Report, the American Association of Collegiate Registrars and Admissions Officers.
[2] The term "universities" will be used to include both colleges and universities.
[3] Region III consists of: Delaware, Maryland, Pennsylvania, Virginia, West Virginia and the District of Columbia.

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

RESULTS OF REVIEW

During our review, all 12 of the universities reported taking steps or making plans to limit SSN use. For example, none of the 12 universities displayed the SSNs on students' identification cards. However, at the time of our review, 5 of the 12 universities used the SSN as the primary student identifier. As such, students at these five universities may have been subject to a higher potential for identity theft and fraud. We identified incidences of identity theft at two of these universities. A third university experienced a break-in of a computer system containing SSN information. Further, 2 of the 12 universities used postcards for prospective students that requested SSN information. The unnecessary use of SSNs increased the potential for individuals to illegitimately gain access to these numbers and misuse them, thus creating SSN integrity issues.

UNIVERSITIES REPORT TAKING STEPS OR MAKING PLANS TO LIMIT SSN USE

All 12 of the universities reported taking steps or making plans to limit using SSNs as student identifiers. While we found the universities' admission applications[4] requested students' SSNs, the universities reported this information was needed for financial aid applications and payroll. However, none of the 12 universities displayed the SSNs on students' identification cards.

Of the 12 universities reviewed, 7 reported assigning their students alternate identification numbers. Students, faculty, and staff use these numbers for most university transactions. Students' SSNs remain in the universities' databases as secondary identifiers. The institutions exercised limited use of the students' SSNs. For example, the seven universities used SSNs when it was necessary to verify students' identities, process financial aid applications, and report wages of student employees. The remaining five universities reported plans to assign their students alternate identification numbers in the future.

Further, 4 of the 12 universities had taken actions to decrease the risk of improper SSN disclosure. These universities required that personnel handling documents containing confidential information sign a disclosure statement (see Appendix D). Some of the documents we reviewed contained references to the Family Educational Rights and Privacy Act and the fact that the handler of such documents may be subject to criminal prosecution and civil penalties, as well as disciplinary action by their employer if they improperly disclose confidential information. We believe the use of disclosure statements can decrease the risk of improper disclosure of SSNs. The remaining eight universities did not report use of disclosure statements.

[4] Admission applications refer to applications available in the traditional paper or electronic formats.

SOME UNIVERSITIES USED SSNs AS PRIMARY STUDENT IDENTIFIER

We found that 5 of the 12 universities used the SSN as the primary student identifier. As such, students at these universities may have been subject to a higher potential for identity theft and fraud. These five universities used SSNs for a variety of purposes. For example, we found four universities used students' SSNs for class registration and displayed students' SSNs on class rosters. In addition, one university displayed students' SSNs on grade reports, two universities used the SSN for student "computer log-ons,"[5] and three universities displayed the SSN on unofficial transcripts. Further, one university incorporated students' SSNs in the coding used for identification cards. Using specialized equipment, persons not authorized to access students' information may be able to identify students' SSNs in the coding.

For these types of activities, the universities could use other means to identify students. For example, they could use an alternate student identification number, as we noted is being done at other universities. Using an alternate identifier could reduce the risk of unauthorized disclosure of SSNs. Officials at the five universities indicated the SSN was used as the primary student identifier because of computer system requirements, common historical practice, convenience, and identity verification. Officials at all five universities reported plans to reduce use of the SSN, where possible, within the next 2 years. The universities plan to use an alternate number as the primary student identifier.

Several states have enacted laws that place certain restrictions on universities' use of SSNs.[6] However, in states without such laws, universities should limit their collection and use of student SSNs to minimize the potential for SSN misuse.

POTENTIAL RISKS ASSOCIATED WITH COLLECTING AND USING SSNs

Universities' collection and use of SSNs can increase the risk of identity theft and fraud. 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. During our review, we identified incidences of identity theft that occurred at two universities. A computer system containing SSN information was compromised at a third university. In addition, we found two universities used postcards requesting SSN information for prospective students.

At one of the five universities that used the SSN as the primary student identifier, an employee was arrested and charged with six counts of identity theft.

---

[5] A computer log-on is used to establish communication and initiate interaction with a time-shared computer or network.

[6] Arizona, New York, Maryland, Rhode Island and Wisconsin are among those states that have enacted laws impacting college and university SSN use.

In September 2004, local police reported this employee worked in the office handling students' registrations and allegedly used that access to collect student information. Police further alleged the employee provided students' personal information to an accomplice. An university official acknowledged the employee copied personal information, such as SSNs and credit card numbers. Ultimately, the employee and accomplice were allegedly able to wire themselves cash using the credit card accounts of at least six people. Although we did not determine the extent unauthorized disclosure of students' SSNs contributed to this incident, such disclosures can contribute to identity theft, fraud or other illegal activities associated with SSN misuse.

The second incident involved identity theft by a student who allegedly obtained instructors' SSNs to change her grade. An university official reported a student purchased online the SSNs of two teachers and posed as the teachers to change failing grades. The university's website indicated the student "…posed as an instructor who wanted to change her password over the phone. She played on the good graces of a university staff member, who, trying to be helpful made the change, thus enabling the student to assume a faculty identity and attempt to change her information in two courses. In another instance, she guessed a faculty member's password and attempted to make a grade change." Although we did not determine the extent university policies concerning the use of instructors' SSNs contributed to this matter, this incident demonstrates the potential harm that can occur when SSNs are used to commit identity theft.

After we completed our work at the schools, one university reported computer data had been compromised. Information on the university's website indicated computer hackers illegally accessed a server containing information relating to identification (ID) cards. The ID server contained names, photographs, ID numbers, and SSNs for all individuals who had university identification cards. A university official confirmed that, when the compromise was discovered, the ID server was immediately disconnected from the network. The universities' website indicated no illegal use had occurred, but the data on the server could be used for identity theft. This incident underscores the need for universities to make every attempt to secure students' SSNs.

We also identified a data collection condition that increased the risk of unauthorized disclosure of SSNs. We found two universities used postcards for prospective students that requested SSN information (see Exhibit 1). Both postcards indicated the SSN was optional.

One postcard used a fold-over security flap to prevent viewing. An university official told us this measure was taken in response to students' concerns of identity theft. However, the location of the adhesive seal allowed the prospective students' information to be viewed by pushing the ends of the card together. The other postcard made no attempt to prevent viewing of prospective students' information. Information on both postcards could be viewed by anyone handling the correspondence. If prospective students entered SSNs on the postcards, the SSN and other personal information would be at-risk of unauthorized disclosure.

Exhibit 1: Information on Postcard Requesting Student SSN

PLEASE PRINT

DATE _____ SS# (optional) _____ BIRTHDATE _____
NAME (LAST) _____ (FIRST) _____ (MI) _____
ADDRESS _____
CITY/STATE _____ ZIP _____
E-MAIL ADDRESS _____
HIGH SCHOOL _____YEAR OF HS GRADUATION _____
COLLEGE MAJOR _____

☐ 2-YEAR ☐ 4-YEAR ☐ SKILL-SET ☐ ONE-YEAR CERTIFICATE

HOME TELEPHONE _____COUNTY _____

ETHNICITY (optional) ☐ White, non-Hispanic ☐ American Indian or Alaskan Native ☐ Black, non Hispanic

☐ Asian or Pacific Islander ☐ Hispanic ☐ Other

_____
_____

TRANSFER STUDENT ONLY
INSTITUTION(S) ATTENDED _____

CONCLUSION AND RECOMMENDATIONS

Despite the potential risks associated with using SSNs as primary student identifiers, many universities continue this practice. Universities' collection and use of SSNs can increase the risk of SSN misuse, identity theft, and fraud. We recognize the Agency's challenge of educating such a large number of universities to the potential risks that exist when SSNs are collected and used. However, given the potential threats to SSN integrity, such a challenge should not discourage SSA from taking appropriate and feasible steps to safeguard SSNs. Given the potential risks for SSN misuse and identity theft, we believe SSA can better safeguard SSN integrity by educating universities about unnecessary SSN use.

Accordingly, we recommend that the Regional Commissioner:

1. Extend outreach efforts when possible through public information sources such as the regional website, pamphlets, etc., to encourage universities to limit their collection and use of SSNs.

2. Encourage universities to require a disclosure statement from employees acknowledging they understand the documents they review and use are confidential, and that improperly releasing confidential information could subject the employee to disciplinary and other legal actions.

3. Promote the best practices of universities that no longer use SSNs as primary student identifiers.

AGENCY COMMENTS

SSA agreed with the intent of all our recommendations and is taking corrective action. The full text of SSA's comments is included in Appendix E.

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)) 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 (FERPA) (20 U.S.C. § 1232g; 34 C.F.R. Part 99) 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.

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)).

[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 these rights are referred to as "eligible students."

Scope and Methodology

To accomplish our objective, we:

- selected 2 universities from each of the 5 States in Region III and Washington, DC—1 university with more than 15,000 students, and 1 university with fewer than 15,000 students;
- interviewed selected university personnel responsible for student admissions/registrations;
- reviewed Internet websites of 12 colleges and universities we visited;
- reviewed applicable laws and regulations; and
- reviewed selected articles, reports and a study regarding universities' use of Social Security numbers as student identifiers.

We visited 12 educational institutions and interviewed personnel to learn more about their policies and practices for using Social Security numbers 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 Social Security numbers. The Social Security Administration entity reviewed was the Office of the Deputy Commissioner for Operations. We conducted our audit from September through November 2004 in accordance with generally accepted government auditing standards.

Educational Institutions Contacted

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

	Institution	Location	Student Enrollment
1	Delaware State University	Dover, Delaware	3,367
2	University of Delaware	Newark, Delaware	18,998
3	Community College of Baltimore County	Baltimore, Maryland	13,953
4	Towson University	Towson, Maryland	16,705
5	Shippensburg University	Shippensburg, Pennsylvania	7,347
6	Community College of Philadelphia	Philadelphia, Pennsylvania	18,537
7	Fairmont State University	Fairmont, West Virginia	5,966
8	West Virginia University	Morgantown, West Virginia	22,201
9	Lynchburg College	Lynchburg, Virginia	1,874
10	George Mason University	Fairfax, Virginia	25,427
11	Gallaudet University	Washington, D.C.	1,558
12	Catholic University of America	Washington, D.C.	4,473

Source: We determined student enrollment by reviewing university websites or the following website: www.collegeboard.com/splash

Information on Confidentiality Disclosure

STUDENT WORKER STATEMENT OF UNDERSTANDING OF THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

I understand that by the virtue of my employment with the _____Office at University, I may have access to records, which contain individually identifiable information, the disclosure of which is prohibited by the Family Educational Rights and Privacy Act. I acknowledge that I fully understand that the intentional disclosure by me of this information to any unauthorized person could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure also violates _____ University's policy and could constitute just cause for disciplinary action including termination of my employment regardless of whether criminal or civil penalties are imposed.

Date: Student Worker's Signature

Agency Comments

March 16, 2005

OIG DRAFT REPORT, USE OF SSNs AS STUDENT IDENTIFIERS IN THE PHILADELPHIA REGION, AUDIT NO. 22004096 - INFORMATION

GENERAL COMMENTS:

Although the recommendations in the audit report resulted from practices of universities in our region, it is clear that the use of SSNs as student identifiers is a concern nationwide. We are also aware that a similar audit conducted in Region IV produced nearly identical recommendations. It is unclear whether you will be consolidating all of the regional audit reports into a national report, but we suggest that this be considered to address our belief that full implementation of the recommendations will require contacts and coordination beyond the regional level.

RECOMMENDATION 1:

Extend outreach efforts when possible through public information sources such as the regional website, pamphlets, etc., to encourage universities to limit their collection and use of SSNs.

COMMENTS:

In our ongoing contacts with local universities, we will continue to make them aware of Social Security's goal of ending the use of the SSN as a student identifier. In the course of our normal recruitment activities, we will include reminders to administration officials that the SSN should not be used as a student identifier. In our upcoming national recruitment conference call, we will suggest to all regions that this issue become a standard part of our recruitment contacts. We will also include this topic in our Public Affairs Specialists' portfolio for inclusion in appropriate settings.

RECOMMENDATION 2:

Encourage universities to require a disclosure statement from employees acknowledging they understand the documents they review and use are confidential, and that improperly releasing confidential information could subject the employee to disciplinary and other legal actions.

COMMENTS:

While we agree with the recommendation, we believe that this should be dealt with on a national level. Presumably, the Agency would want consistency among universities in

terms of standard language that should be included on a disclosure statement. At the regional level we will suggest in our contacts with all employers that their employees be made aware of the confidentiality issues involved whenever an SSN is part of a record.

RECOMMENDATION 3:

Promote the best practices of universities that no longer use SSNs as primary student identifiers.

COMMENTS:

The draft report does indicate that most institutions are already moving in this direction. A compilation of best practices would be most effective if we gather information from universities across the country. The activity that is required to implement this recommendation, to poll universities for their best practices and develop a mechanism for promoting them, also appears to be a directive that would best be performed at a national level. In the Philadelphia region we can begin this process by compiling a list of experiences and suggestions from those universities who have made the transition from use of the SSN to some other form of identification.

If members of your staff have any questions regarding these comments, they may contact Carla White of the Center for Program Support at 215-597-1124.

/s/
Laurie Watkins

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

Walter Bayer, Director, Mid-Atlantic Audit Division (215) 597-4080

Randy Townsley, Audit Manager, General Management (410) 966-1039

Michael Maloney, Audit Manager, Mid-Atlantic Audit Division (703) 578-8844

Cylinda McCloud-Keal, Audit Manager, Mid-Atlantic Audit Division (215) 597-0572

Acknowledgments

In addition to those named above:

Ehab Bestawrose, Senior Auditor

Alan Carr, Senior Auditor

Eugene Crist, Auditor

Virginia Montelpare, Auditor

Ellen Silvela, Auditor

Kimberly Beauchamp, Writer-Editor

For additional copies of this report, please visit our web site at http://ww.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-13-05-15083

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

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.