



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF INSPECTOR GENERAL

OCT 31 2002

CONTROL NUMBER
ED-OIG/A19-C0006

Theresa S. Shaw, Chief Operating Officer
Federal Student Aid
U.S. Department of Education
830 First Street, NE
Washington, DC 20202

Dear Ms. Shaw:

This **Final Audit Report** (Control Number ED-OIG/A19-C0006) presents the results of our audit of the Department of Education's controls over the access, disclosure, and use of Social Security Numbers (SSNs) by third parties.

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by appropriate Department of Education officials.

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available, if requested, to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

BACKGROUND

The Social Security Administration created the Social Security Number (SSN) in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. Over the years, the SSN has become a national identifier used by Federal agencies, State and local governments, and private organizations. Due to concerns related to sharing of personal information and identity theft, Congress asked the General Accounting Office (GAO) to study how and to what extent, Federal, State and local government agencies use individuals' SSNs and how these entities safeguard records or documents containing those SSNs. The Chairman of the House Ways and Means Subcommittee on Social Security asked the Social Security Administration, Office of Inspector General, and the

President's Council on Integrity and Efficiency (PCIE) to review the way Federal agencies disseminate and control the SSN. The Offices of Inspector General (OIG) for several agencies participated in this review.

A standardized audit approach was developed for all participating agencies based on a GAO survey conducted in August 2001. GAO sent questionnaires to officials of Federal programs that were likely to routinely collect, maintain, and use individuals' SSNs. GAO asked each agency to complete questionnaires for five program areas. Each OIG participating in the PCIE effort was asked to conduct an in-depth review of one of the programs for which a questionnaire was completed. The Department of Education (Department) completed questionnaires for the following areas: Direct Loan Originations, Pell Grant Program, Federal Student Aid Collections, Education Central Automated Processing System/Grants and Administration Payment System (EDCAPS/GAPS), and Rehabilitation Services. We selected the Pell Grant Program for the PCIE review since the Department reported the highest number of SSNs in that program.

The objectives were to determine whether each agency:

1. Makes legal and informed disclosures of SSNs to third parties;
2. Has appropriate controls over contractors' access and use of SSNs;
3. Has appropriate controls over other entities' access and use of SSNs; and
4. Has adequate controls over access to individuals' SSNs maintained in its databases.

AUDIT RESULTS

Our audit was limited to review of the Pell Grant program and the Recipient Financial Management System (RFMS). We determined that the only disclosures of SSNs to third parties from the RFMS were to Federal Student Aid (FSA) contractors. As such, the third objective regarding access by other entities was not applicable. (See the Objectives, Scope, and Methodology section of this report for the definition of a disclosure established for this review and the audit scope. See also Attachment 1 for details on the flow of SSNs through the Pell Grant system.)

We found that in general, the Department made legal and informed disclosures of SSNs. We found that improvements were needed in the Department's controls over contractors' access to and use of SSNs, and in controls over access to individuals' SSNs maintained in the RFMS.

The Department responded to our draft report, concurring with the finding and all recommendations provided. The Department also described specific corrective actions

they have taken and intend to take to address the issues noted. The full text of the Department's response is included as Attachment 2 to this audit report.

Finding No. 1 Improvements Are Needed in Monitoring of FSA Contractor Access, Disclosure and Use of Social Security Numbers.

Our audit revealed FSA staff did not adequately monitor the RFMS contractor's performance to ensure that SSNs were appropriately safeguarded. Specifically, we found that FSA staff did not confirm whether the RFMS contractor provided Privacy Act training for contractor personnel as required, and whether all contractor staff with access to the RFMS were still currently employed by the contractor.

We also found that FSA did not maintain a current listing of RFMS users. During our review, FSA staff provided us with a listing of staff with access to the system, but they stated that the listing needed to be updated. FSA staff further stated that the RFMS contractor previously provided regular reports of all current users, but that such a report had not been provided since June 2002.

The Privacy Act of 1974, (5 U.S.C. § 552a, as amended), provides requirements on the protection of personal information. Sections (e)(9) and (e)(10) of the Act require agencies to:

[E]stablish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.

[E]stablish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Section (m)(1) of the Privacy Act requires agencies to include compliance with the Privacy Act in contracts for the operation of a system of records. Likewise, the Federal Acquisition Regulation (FAR) § 24.102(a) states that the Privacy Act:

[R]equires that when an agency contracts for the design, development, or operation of a system of records on individuals on behalf of the agency to accomplish an agency function the agency must apply the requirements of the Act to the contractor and its employees working on the contract.

The Department's Directive (Directive), C:GPA 2-110, "Contract Monitoring for Program Officials," dated January 12, 1987, establishes internal standards and guidelines in conducting day-to-day contact monitoring. The Directive states:

It is the policy of the Department of Education (a) to monitor every contract to the extent appropriate to provide reasonable assurance that the contractor performs the work called for in the contract, and (b) to develop a clear record of that performance and the Department's efforts in monitoring it. (Section II, page 2 of the Directive)

Contract monitoring is conducted by the Government to ensure that the contractor performs according to the specific promises and agreements that make up the contract. (Section VIII.A, page 10 of the Directive)

Site visits may be advisable for particularly complex contracts, for those known to be experiencing performance difficulties, or for any contract where it would be good to demonstrate the Government's interest or concern for successful performance. (Section H.1, page 22 of the Directive)

The RFMS contract Statement of Work, Section 5.8.3, Computer Security and Privacy Act Training, states that the contractor shall:

Provide formal classroom instruction for contractor personnel and packaged instruction for Department of Education staff prior to system start-up....Give computer security and Privacy Act refresher training annually to meet the requirements identified in the Computer Security Act of 1987.

We found that FSA included the requirements of the Privacy Act in the RFMS contract and established rules of conduct for the system. However, FSA staff did not conduct site visits or otherwise verify that the contractor was complying with the Privacy Act requirements. For example, FSA did not monitor contractor activities to ensure that training was provided as required. FSA staff did not receive copies of training records or certifications from the contractor that training had taken place to confirm that these requirements were being met. In fact, annual refresher training had not been provided since November 2000. We also found that FSA staff did not maintain a current listing of RFMS users or validate such a listing to ensure all users were appropriately trained and were still employed by the contractor.

As a result, FSA does not have assurance that contractor staff with access to SSNs and other personal information in the RFMS are aware of Department policies and procedures and Federal laws prohibiting the disclosure of such information. FSA also does not have assurance that contractor staff with access to the system are still current employees.

Recommendations:

We recommend that the Chief Operating Officer for Federal Student Aid take actions to ensure:

- 1.1 FSA staff appropriately monitor contractor operations to ensure that training is provided to contractor staff as required.
- 1.2 FSA staff receive copies of training records or certifications from the contractor on a regular basis and periodically reconcile this information with user listings to ensure all users are appropriately informed of their responsibilities and the prohibitions against disclosure of SSNs and other information.
- 1.3 FSA maintains a current listing of RFMS users and periodically validates the listing of RFMS users to ensure that all staff with access to the system are current employees, and that access is canceled timely for staff that have separated.
- 1.4 FSA review other contracts with Privacy Act provisions to ensure that those contracts are appropriately monitored for compliance with Privacy Act requirements.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objectives of our audit were to determine whether the Department:

1. Makes legal and informed disclosures of SSNs to third parties;
2. Has appropriate controls over contractors' access and use of SSNs;
3. Has appropriate controls over other entities' access and use of SSNs; and
4. Has adequate controls over access to individuals' SSNs maintained in its databases.

For the purpose of this audit, disclosure of SSNs was defined as new information provided to a third party, whether it be another Government agency, a contractor, or an outside organization. If a third party first sends a file of SSNs to the agency, the agency matches those SSNs against its records to determine eligibility or some other information, and sends the additional information back to the third party, that process is not considered a disclosure for the purposes of our audit. For example, the exchange of information between educational institutions and the RFMS is not considered a disclosure, since the institutions provide the SSN with records initially sent to RFMS. Applying this criterion, we determined that SSNs were not disclosed from the RFMS to entities other than contractors. As such, the third objective of this audit did not apply to the scope of our

audit. See Attachment 1 for further details on the flow of SSNs through the Pell Grant system.

In selecting a program to review, we performed an analysis of the Department's responses to the GAO questionnaire for Direct Loan Originations, Pell Grant Program, Federal Student Aid Collections, EDCAPS/GAPS, and Rehabilitation Services. We evaluated the Department's responses regarding the volume of records stored on computer systems, the disclosure of SSN information to third parties, the number of private contractors who have access to SSN information, computer network access by third parties, and the number of separate computer systems that contain SSNs. We selected the Pell Grant Program for further review based on the Department's report of approximately 50 million SSNs in the system. This amount far exceeded those reported for the other programs. The other factors reviewed did not differ significantly among the five programs.

The scope of our audit was calendar year 2001. We did not review the Common Origination and Disbursement system that is now used for the Pell Grant Program, as that system had not been implemented during the audit period.

To accomplish our objectives, we conducted interviews with FSA staff responsible for the operation and security of the Pell Grant system. We reviewed the Privacy Act of 1974, Federal Acquisition Regulation, and Departmental policies and procedures on the protection and use of Privacy Act information and on the requirements for contract monitoring. We reviewed the general terms and conditions for the contracts for development and operation of the RFMS to determine the requirements regarding access to and disclosure of SSNs. We also reviewed the Department's Privacy Act System of Records notices for RFMS and other related FSA systems. We reviewed disclosures of the uses of data made on the Free Application for Federal Student Aid (FAFSA) form and the FAFSA electronic form on FSA's website. We reviewed computer-matching agreements with other Federal agencies, as well as risk assessments and security reviews conducted of the RFMS and of the Virtual Data Center where RFMS data is stored. We did not rely upon computer-processed data in conducting our audit.

We performed our fieldwork at applicable Department of Education offices in Washington, DC, during the period April 2, 2002, through September 18, 2002. We held an exit conference with Department officials on September 18, 2002. We performed our audit in accordance with generally accepted government auditing standards appropriate to the scope of the review described above.

STATEMENT ON MANAGEMENT CONTROLS

We made a study and evaluation of Federal Student Aid's management control structure over the access, disclosure, and use of Social Security Numbers by third parties. Our review was limited to evaluation of the Pell Grant system operations during the period of our review. Our study and evaluation was conducted in accordance with generally accepted government auditing standards.

For the purpose of this report, we assessed and classified the significant management control structure into the following categories:

- Disclosure of SSNs to third parties,
- Contractors' access and use of SSNs, and
- Access to SSNs in the Department's RFMS database.

Department management is responsible for establishing and maintaining a management control structure. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control procedures. The objectives of the system are to provide management with reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or disposition and that the transactions are executed in accordance with management's authorization and recorded properly, so as to permit effective and efficient operations.

Because of inherent limitations in any management control structure, errors, or irregularities may occur and not be detected. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions, or that the degree of compliance with the procedures may deteriorate.

Our assessment disclosed conditions in the Department's management control structure over disclosure of SSNs to contractors, which, in our opinion, result in more than a relatively low risk that errors, irregularities, and other inefficiencies may occur resulting in inefficient and/or ineffective performance. We noted a weakness with respect to the Department's monitoring of contractor's access to, disclosure, and use of SSNs, and in controls over access to individuals' SSNs in the RFMS. These weaknesses are discussed in the **Audit Results** section of this report.

ADMINISTRATIVE MATTERS

Please provide the Supervisor, Post Audit Group, Office of the Chief Financial Officer and the Office of Inspector General with quarterly status reports on promised corrective actions until all such actions have been completed or continued follow-up is unnecessary.

We appreciate the cooperation provided to us during this review. Should you have any questions concerning this report, please call Michele Weaver-Dugan at (202) 863-9526. Please refer to the control number in all correspondence related to the report.

Sincerely,

A handwritten signature in cursive script that reads "Helen Lew". The signature is written in black ink and is positioned above the printed name.

Helen Lew

Acting Assistant Inspector General for Audit Services

Attachment 1**The Flow of Social Security Numbers (SSNs)
through the Pell Grant System**

- Applicant SSNs are originally provided on the Free Application for Federal Student Aid (FAFSA) Application Processing System. The Recipient Financial Management System (RFMS) receives the SSNs for eligible Pell recipients via the Eligible Applicant File from the Central Processing System (CPS).
- The Federal Pell Grant program does not directly make disclosures to eligible applicants of the uses of their personal information. Such disclosures do appear on the FAFSA forms (paper and electronic), Privacy Act Systems of Records notices, and Federal Register. These notices are applicable to all Title IV applicants, including Pell eligible applicants.
- Institutions send origination records to RFMS. These origination records include students' SSNs and institutions' determinations of the Pell award amount. Original SSNs are matched to the eligible applicant data provided previously to RFMS by CPS. RFMS processes the data received from the institution and then provides the institution with an acknowledgment indicating that the record has been accepted, corrected, or rejected.
- Once origination records have been accepted, institutions disburse funds to the students and transmit disbursement records to RFMS for processing. Again, students' SSNs are provided to RFMS by institutions in disbursement records. RFMS matches the information provided by institutions to the previously received origination records and transmits acknowledgements back to institutions.
- Upon request by an institution, a year-to-date summary of originations and disbursements information that the institution previously sent to RFMS will be provided. This file includes only accepted and/or corrected records previously sent by the institution.



Attachment 2

UNITED STATES DEPARTMENT OF EDUCATION
STUDENT FINANCIAL ASSISTANCE
WASHINGTON, D.C. 20202-5132

CHIEF OPERATING OFFICER

OCT 23 2002

Ms. Michele Weaver-Dugan
Director, Operations Internal Audit Team
U.S. Department of Education
Office of Inspector General
400 Maryland Avenue, S.W.
Washington, DC 20202-1600

Dear Ms. Weaver-Dugan:

Thank you for the opportunity to review and comment on the draft audit report (Control Number ED-OIG/A19-C0006) that presents the results of your audit of the Department of Education's "Controls over the Access, Disclosure, and Use of Social Security Numbers (SSNs) by Third Parties." Specifically, your audit finding and the recommendations pertain to your audit of the Federal Pell Grant program and the Recipient Financial Management System (RFMS) administered by the Department's Federal Student Aid program.

We concur with the finding and the four recommendations identified in the report. The attachment provides the Department's response to each recommendation. We used your report to assist us in improving our controls over Social Security Number access, disclosure, and release.

Again, we appreciate the opportunity to review and comment on the draft report.

Sincerely,

A handwritten signature in blue ink, appearing to read "Theresa S. Shaw".

Theresa S. Shaw

cc: Kathleen Wicks
Rosemary Beavers

**Response to OIG Draft Audit Report
Audit of Controls over the access, disclosure,
And use of Social Security Numbers (SSNs)
by third parties**

Office of Inspector General (OIG) draft report section:

OIG Finding No. 1:

Improvements are needed in monitoring of FSA Contractor Access, Disclosure and Use of Social Security Numbers.

OIG Recommendation 1.1: Ensure FSA staff appropriately monitor contractor operations to ensure that training is provided to contractor staff as required.

FSA Response: We concur. The Contractor has scheduled Privacy Act training for October 24, 2002. Once the training is completed, the Systems Security Officer (SSO) will obtain a report from the contractor. The SSO will monitor the contractor more closely and receive compliance reports on a monthly basis for the full term of the contract. The RFMS contract is scheduled to end this fiscal year. We will ensure that the SSO for the Common Origination and Disbursement (COD) contract, which replaces RFMS, complies with the Privacy Act and Departmental Directive C: GPA 2-110, "Contract Monitoring for Program Officials" and appropriately monitors contractor operations to ensure that training is provided to contractor staff.

OIG Recommendation 1.2: Ensure FSA staff receive copies of training records or certifications from the contractor on a regular basis and periodically reconcile this information with user listings to ensure all users are appropriately informed of their responsibilities and the prohibitions against disclosure of SSNs and other information.

FSA Response: We concur. On October 24, 2002, the Contractor has scheduled Privacy Act training that will appropriately inform all users of their responsibilities and prohibitions against disclosure of SSNs and other information. The Contractor will submit training records or certifications of training upon completion of this training. The RFMS contract is scheduled to end this fiscal year. We will ensure that the SSO for the COD contract monitors the contract more closely and on a monthly basis, and reconciles the training records with the user listing.

OIG Recommendation 1.3: Ensure FSA maintains a current listing of RFMS users and periodically validates the listing of RFMS users to ensure that all staff with access to the system are current employees, and that access is canceled timely for staff that have separated.

FSA Response: We concur. In October 2002, the SSO reviewed and validated the listing of RFMS users to ensure that they are current employees. The SSO confirmed that access was canceled for employees who separated. The RFMS contract is scheduled to end this fiscal year. We will ensure the SSO for the COD contract reviews and validates listings on a monthly basis and removes employees upon notification of separation.

OIG Recommendation 1.4: *Ensure FSA review other contracts with Privacy Act provisions to ensure that those contracts are appropriately monitored for compliance with Privacy Act requirements.*

FSA Response: We concur. We will have SSO's review all current contracts with Privacy Act provisions to ensure that they are appropriately monitored for compliance with Privacy Act requirements.