United States General Accounting Office

GAO

Report to the Chairman, Committee on Governmental Affairs, U.S. Senate

September 2002

INFORMATION MANAGEMENT

Selected Agencies' Handling of Personal Information

GAO-02-1058

GAO
Accountability★Integrity★Reliability

Highlights

INFORMATION MANAGEMENT Selected Agencies' Handling of Personal Information

Highlights of GAO-02-1058, a report to the Chairman, Committee on Governmental Affairs, U.S. Senate

Why GAO Did This Study

To obtain government services, members of the public must often provide agencies with personal information, which includes both identifying information (such as a name or Social Security number, which can be used to locate or identify someone) and nonidentifying information (such as age or gender). GAO was asked to review agencies' handling of the personal information they collect and whether this handling conforms with federal law, regulation, and agency guidance.

What GAO Found

GAO reviewed the processes used in handling personal information collected from the public on forms at four different agencies—Agriculture, Education, Labor, and State. These four agencies were chosen because their forms represent a range of characteristics, including the time needed to fill them out (the total paperwork burden hours) and the purpose of the information they collect. In reviewing these forms, GAO concentrated on four areas (information collection, privacy, security, and records management).

Handling of personal information varied among the agencies studied. Overall, agencies collected a substantial amount of personal information of a wide variety of types, including personal identifying information (names and Social Security numbers) and demographic, financial, and legal data (see display below). Agency procedures for handling personal information collected were complex, involving numerous processes and a wide range of personnel with access to the information. The personal information collected was shared extensively with other federal agencies, other government entities (state, local, tribal, and foreign), and private individuals and organizations through authorized procedures.

The agencies generally complied with the key requirements and guidance pertaining to information collection, privacy, security, and records management. However, GAO identified isolated instances of forms that were not accurate or current; other forms did not contain the proper privacy notices.

What GAO Recommends

To strengthen agency compliance with requirements for handling personal information, GAO recommends that the Secretary of Labor ensure that data collection forms are up to date and include appropriate Privacy Act and other notices. GAO also recommends that the Secretary of Agriculture ensure that the notices of how the department shares forms data be assessed and forms updated as appropriate.

Labor, Agriculture, Education, and State officials generally agreed with GAO's report. In addition, Labor officials posted a valid, up-to-date form as recommended.

Agencies Collect Many Types of Personal Information

Information about
Individual applicant
Spouse
Children
Dependents
Parents

Personal identifiers
Legal name
Maiden name
Aliases
Home phone number
Business phone number
Social Security number
Driver's license number
Alien registration number
Legal address
E-mail address

Demographic data
Date of birth
Place of birth
Citizenship
Marital status
Date of marriage/divorce
Number in household
Education level
Occupation
Gender
Physical attributes, e.g., height, eye color

Financial/legal data
Salary
Investments
Net worth
Credit history
Child support
Bankruptcy
Criminal record
Drug convictions
Litigation

Source: GAO analysis.

Contents

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

September 30, 2002

The Honorable Joseph I. Lieberman
Chairman, Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

The security and protection of personal information[1] is a topic of growing national concern. Personal information is provided to the government by the public for a specific purpose—to receive a government benefit, obtain a service or loan, or participate in a program. However, this information in the hands of unauthorized persons can present a risk to those who provide it—such as misuse of personal information or loss of personal privacy.

This report addresses the flow and management of personal information at four agencies: the Departments of Agriculture, Education, Labor, and State. At your request, we selected one information collection[2] form requesting personal information at each of these agencies, to review its life cycle from collection, use, dissemination, and storage, through archiving and/or disposal. As agreed with your office, our objectives were to (1) document the flow of and practices associated with the handling of personal information within these agencies and (2) evaluate these information flows and practices against agency and federal guidance.

To fulfill our objectives, we modeled the data flows for each of these forms. We conducted structured interviews with top agency officials and program managers to understand the data flow and agency practices. We also reviewed applicable laws and regulations and analyzed agency documentation on policies and procedures for using, protecting, making available, and disposing of this information. We conducted our review from March 2001 to July 2002, in accordance with generally accepted government auditing standards.

[1] Personal information is defined as all information associated with an individual and includes both identifying information (e.g., name, Social Security number, E-mail address, and agency-assigned case number) and nonidentifying information (e.g., age, finances, and gender).

[2] Collections of information include (1) requests for information for transmission to the government, such as application forms and written report forms; (2) record keeping requirements; and (3) third party or public disclosure requirements.

On August 19, 2002, we provided a detailed briefing[3] to your office on the results of our work. The briefing slides are included as appendix I, and a detailed discussion of objectives, scope, and methodology is included as appendix II. The purpose of this report is to provide the published briefing slides and appendixes to you and to officially transmit our recommendations to the Secretaries of Labor and Agriculture.

In brief, we reported that these four agencies' handling of personal information varied greatly—including the types and amount collected—and a wide range of personnel had access to the information. Further, these agencies generally followed the applicable laws and regulations in the collections we reviewed, and the agency officials recognized the need to protect this information. We did, however, note isolated instances of forms that were not accurate or current, and other forms that did not contain the proper privacy notices.

Recommendations

In order to meet the requirements of the Privacy Act and other relevant laws and guidance protecting personally identifiable information, we recommend that the Secretary of Labor ensure that the appropriate agency officials review their data collection forms to ensure that the electronic forms (1) include the Paperwork Reduction Act and Privacy Act statements and all notices, as appropriate; and (2) are valid and up to date. We also recommend that the Secretary of Agriculture ensure that Agriculture officials periodically determine that notices of how they share personal information from their data collections are still valid (updating their forms as appropriate).

Agency Comments

In providing oral comments on a draft of this report, officials at Labor, State, Agriculture, and Education—including the Assistant Secretary for Employment Standards at Labor, the Director of Information Management and Liaison at State, and representatives from the offices of the Chief Information Officers at Agriculture and Education—generally agreed with our results. Officials also provided technical comments that we incorporated as appropriate. In addition, Labor noted that, as we recommended, they have now posted a valid, up-to-date electronic

[3] We have amended the briefing as of September 12, 2002, to include technical corrections and suggestions provided by the agencies.

employee compensation form on their Web site, which includes the required Paperwork Reduction Act and Privacy Act statements.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies to the Secretaries of the Departments of Agriculture, Education, Labor, and State; the Director of the Office of Management and Budget; and other interested congressional committees. Copies will also be available at no charge on our Web site at www.gao.gov.

Should you have any questions on matters contained in this report, please contact me at (202) 512-6240, or by E-mail at koontzl@gao.gov. Other key contributors to this report included Elizabeth Bernard, Tonia Brown, Barbara Collier, Patricia Fletcher, Katherine Howe, Michael Jarvis, Colleen Phillips, David Plocher, and Warren Smith.

Sincerely yours,

Linda D. Koontz
Director, Information Management Issues

Selected Agencies' Handling of Personal Information

Selected Agencies' Handling of Personal Information

Briefing for Staff

Committee on Governmental Affairs
United States Senate

August 15, 2002

As amended September 12, 2002

Briefing Outline

- Background
- Summary of Objectives, Scope, and Methodology
- Results in Brief
- How Agencies Handle Personal Information
- Agencies' Handling of Personal Information Is Generally Adequate
  - Information Collection
  - Privacy
  - Security
  - Records Management

2

Briefing Outline (cont'd)

- Conclusions
- Recommendations
- Agency Comments and Our Evaluation

3

Background
Personal Information

Personal information is all information associated with an individual and includes both identifying information (which can be used to locate or identify an individual) and nonidentifying information.

- *Identifying information* includes name, aliases, Social Security number, E-mail address, driver's license identification number, and agency-assigned case number.
- *Nonidentifying* personal information includes age, education, finances, physical attributes, and gender.

In order to obtain government services or fulfill government obligations—such as obtaining Medicare payments, applying for small business loans, and paying taxes—individuals often must provide government agencies detailed personal information about themselves, their spouses, dependents, and parents.

4

Background
Personal Information

Widespread use of computerized recordkeeping and growth in the use of the Internet to collect and share information have resulted in public concern about the privacy of personal information collected by the government. These concerns include those related to the government's ability to ensure the accuracy and confidentiality of information about individuals and prevent misuse of personal information. For example:

- A 2001 survey from the Information Technology Association of America noted that a majority of Americans believe that business does a better job of protecting their information than does their government, and that Americans are concerned (81%) that their government-held personal data may be misused.
- In a September 2000 study sponsored by the Council for Excellence in Government, by more than two to one, Americans want to proceed slowly (65%) rather than quickly (30%) in implementing e-government because of concerns about security, privacy, and access.
- In the same survey, Americans expressed serious concern about the potential for government employees to misuse personal information (55%) and the general potential for less personal privacy (53%).

5

Background
Laws and Guidance for Managing Personal Information

The Paperwork Reduction Act (PRA) recognized that information is a valuable government resource and must be appropriately managed throughout its life cycle, from its collection to final disposition, whether destruction or preservation. The act also includes specific requirements for managing the collection of information at federal agencies. Other laws and guidance (such as the Privacy Act of 1974, the Computer Security Act, and the Federal Records Act), when combined with the PRA, describe the life cycle framework for information management.

The Privacy Act of 1974 is the primary act regulating the federal government's use of personal information. It places limitations on collection, disclosure, and use of personal information maintained in systems of records by federal agencies.

- A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual.
- One exemption under the act is *routine use*, which permits disclosure of a record to governmental and nongovernmental agencies and individuals for a purpose that is compatible with the purpose for which the information was collected.

.

6

Background

Laws and Guidance for Managing Personal Information (cont'd)

The Computer Matching and Privacy Protection Act of 1988 established safeguards regarding an agency's use of Privacy Act records in performing certain computerized matching programs.

- According to the act, a written *computer matching agreement* is required for any computerized comparison of two or more automated systems of records for the purposes of determining the eligibility of applicants for assistance under federal benefits programs, or of recouping payments or delinquent debts under federal benefits programs. Agreements are also required for any computerized comparison of federal personnel or payroll systems.
- Computer matching agreements must specify the purpose and legal authority for conducting the match and how these matches will be performed.

7

Background

Laws and Guidance for Managing Personal Information (cont'd)

The Computer Security Act of 1987 requires agencies to develop plans for the security and privacy of sensitive information in federal computer systems.

The Government Information Security Reform (GISRA) provisions in the 2001 Defense Authorization Act require agencies to establish risk-based, agencywide information security programs, which must be independently evaluated annually.

The Federal Records Act addresses how agencies manage records, sanctions unlawful removal and/or destruction of records, and provides for submission of permanent records to the Archivist.

Major guidance for the management of personal information is found in

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*;
- National Archives and Records Administration regulations in the U.S. Code of Federal Regulations, Title 36; and
- National Institute of Standards and Technology information security guidance.

8

Objectives, Scope, and Methodology

As agreed with your office, our objectives were to

- determine how agencies are handling personal information collected on selected information collection forms; and
- evaluate the adequacy of agencies' handling of personal information against federal law, regulation, and agency guidance.

9

Objectives, Scope and Methodology (cont'd)

We selected a judgmental sample of four forms with the goal of obtaining a range of the following:

- type of information collected, e.g., demographic, financial, medical;
- collection and submission media, e.g., paper, electronic;
- type of collection, e.g., application for a loan or grant, medical benefits and/or workplace compensation, receipt of a service;
- scope of the system, including computer matching agreements;
- size of the paperwork burden; and
- the categories of individuals providing the information, e.g., farmers, students, federal workers, and the general public.

An additional selection criterion was that the information collected through each form was maintained in a system of records covered by the Privacy Act.

10

Objectives, Scope and Methodology (cont'd)

We chose the following four forms to review:

- Agriculture: Farm Service Agency's "Request for Direct Loan Assistance." The Farm Service Agency provides direct farm ownership, direct farm operating, and emergency loans to qualified farmers. For fiscal year 2001, FSA approved 1,472 farm ownership loans with a value of $163 million, 14,403 operating loans with a value of $690 million, and 1,679 emergency loans with a value of $90 million.
- Education: Office of Federal Student Aid's "Free Application for Federal Student Aid." The Office of Federal Student Aid provides schools and financial institutions with information about a student's financial status and loan/grant eligibility. The Federal Student Aid programs are the largest source of student aid in America, providing over $60 billion a year in grants, loans, and work-study assistance.

11

Objectives, Scope and Methodology (cont'd)

- Labor: Federal Employees' Compensation Program's "Claim for Compensation." The Federal Employees' Compensation Program provides workers' compensation coverage to federal and postal workers for employment-related injuries and occupational diseases. Benefits include wage replacement, payment for medical care, and (where necessary) medical and vocational rehabilitation assistance in returning to work. For fiscal year 2000, this program provided 273,000 workers slightly more than $2 billion in benefits for work-related injuries and illnesses.
- State: Bureau of Consular Affairs' "Application for U.S. Passport." The Bureau of Consular Affairs provides passports for U.S. citizens to travel abroad. In FY 2001, a total of 7.1 million passports were issued.

To determine how agencies are handling personal information, we conducted structured interviews with agency officials and analyzed agency policies and procedures. We used workflow modeling software during sessions with agency officials to describe the steps in the process, the data flows, and who handles the information.

12

Objectives, Scope and Methodology (cont'd)

To evaluate the adequacy of how agencies manage personal information, we focused on information collection, privacy, security, and records management. We reviewed relevant laws and regulations, OMB guidance, and agency procedures. We then compared these requirements and guidance to agency practice.

(Details of our objectives, scope, and methodology can be found in appendix II.)

13

Results in Brief

Handling of personal information varied among the agencies studied and had the following overall characteristics:

- Agencies collected a substantial amount of personal information of a wide variety of types, including personal identifying information (names and Social Security numbers) and demographic, financial, and legal data.
- This information was collected from a range of categories of individuals—farmers, federal employees, students, and citizens seeking to travel abroad.
- Paperwork burden—the time required to fill out each form—ranged from 13 to 60 minutes.
- The personal information collected was shared extensively with other federal agencies, other government entities (state, local, tribal, and foreign), and private individuals and organizations.

Agency procedures for handling personal information collected were complex, involving numerous processes and a wide range of personnel with access to the information.

Results in Brief (cont'd)

The four agencies generally handled personal information adequately in the areas reviewed: information collection, privacy, security, and records management.

- The agencies generally complied with key requirements and guidance in these areas.
- We identified isolated instances of forms that were not accurate or current, and other forms that did not contain the proper privacy notices.

To further strengthen agency compliance with requirements for handling personal information, we are making recommendations to the Secretaries of Labor and Agriculture.

15

How Agencies Handle Personal Information
Data Flow Characteristics

All four forms examined varied in the types of personal information collected, in the categories of individuals supplying the information, in the levels of burden imposed in filling them out, in the processes and personnel involved in their handling, and in the extent of sharing with other entities.

Types of information. For the four forms, agencies collected a substantial amount of personal information of varying types. The following illustrates the types of personal information collected.

Information about
Individual applicant
Spouse
Children
Dependents
Parents

Personal identifiers
Legal name
Maiden name
Aliases
Home phone number
Business phone number
Social Security number
Driver's license number
Alien registration number
Legal address
E-mail address

Demographic data
Date of birth
Place of birth
Citizenship
Marital status
Date of marriage/divorce
Number in household
Education level
Occupation
Gender
Physical attributes, e.g., height, eye color

Financial/legal data
Salary
Investments
Net worth
Credit history
Child support
Bankruptcy
Criminal record
Drug convictions
Litigation

16

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Categories of individuals. Many categories of individuals—farmers, federal employees, students, and U.S. citizens seeking to travel outside the country—provide personal information to request a service, receive a financial benefit, or become eligible for a program of the federal government.

Paperwork burden. As required by the PRA, agencies measure the paperwork burden associated with filling out forms. The burden for these forms ranged from 13 to 60 minutes.

17

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

The following chart provides summary information on the four forms we reviewed.

Agency	Categories of individuals	Burden in minutes[a]
Agriculture	farmers	60 minutes
Education	students	60 minutes
Labor	federal employees	13 minutes
State	U.S. citizens	20 minutes

[a] The amount of time needed to fill out a form is indicated by burden hour estimates, expressed in minutes of time.

18

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Information Sharing. For the four forms we reviewed, the agencies shared personal information extensively with other federal government agencies, other governmental bodies (state, local and tribal), and foreign governments. Information was also shared with private entities including individuals and organizations.

For example, sharing was done (1) as a routine use and (2) under computer matching agreements between agencies.

19

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Routine use with other government agencies

Agency	Agriculture	Education	Labor	State
Courts	x	x	x	
Defense Manpower Data Center	x		x	
Department of Justice	x	x	x	
Department of Labor	x			
Foreign governments				x[a]
HUD	x			
Internal Revenue Service	x			x
Law enforcement agencies (federal, state, local)	x	x	x	x
OMB		x	x	
OSHA			x	
Other governmental bodies			x	x
State agencies		x	x	
U.S. Postal Service	x		x	

[a] State shares information with foreign governments only on limited occasions.

20

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Some examples of routine uses with other government agencies include the following:

- State disclose applicants' mailing addresses to the Internal Revenue Service for the purpose of enabling the IRS to locate such taxpayers to collect taxes and other related tax activities. State also discloses to the IRS names, dates of birth, and Social Security numbers of passport applicants.
- Education discloses personally identifying information, financial data, or expected family contribution data from the applicants to state agencies that have formal agreements with the Secretary of Education for the purposes of coordinating student financial aid.

21

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Routine use with other private entities, both individuals and organizations

Agency	Agriculture	Education	Labor	State
Attorneys	x		x	x
Business firms in specified trade areas	x			
Collection agencies	x		x	
Consumer reporting agencies		x	x	
Contractors providing IT services		x	x	
Credit bureaus			x	
Financial consultants, advisors	x			
Financial/lending institutions	x			
Institutions of postsecondary education		x		
Labor unions			x	
Medical insurance or health plan			x	
Parents, spouses, or immediate families		x		x
Parties involved in litigation		x		
Physicians & other health care providers			x	
Rehabilitation agencies			x	

22

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Some examples of routine use with other entities included the following:

- Agriculture discloses information to lending institutions when it has determined that the farm loan applicant is financially capable of qualifying for credit with or without a guarantee.
- Education may disclose personal information, including financial data, to institutions of postsecondary education to which the applicants have noted that they intend to apply for admission.
- Labor shares information with physicians and other health care providers for the purpose of evaluating and/or treating the claimant for compensation.

23

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Education's Office of Federal Student Aid shared information under computer matching agreements. This office had 11 such agreements with 10 agencies:

- Department of Defense
- Department of Health and Human Services
- Department of Housing and Urban Development
- Department of Justice
- Department of Veterans Affairs
- Immigration and Naturalization Service
- Internal Revenue Service
- United States Postal Service
- Selective Service System
- Social Security Administration (two agreements)

24

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Some of Education's computer matching agreements include matches with

- Department of Justice to determine if the applicant has been convicted of any drug-related offense,
- Department of Veterans Affairs to verify an applicant's veteran status,
- Immigration and Naturalization Service to verify the applicant's entitlement to federal benefits,
- Selective Service System to verify if a male applicant has properly registered for the draft, and
- Social Security Administration to verify an applicant's Social Security number.

25

How Agencies Handle Personal Information
Data Flow Characteristics (cont'd)

Labor shared information under computer matching agreements with the Office of Personnel Management (OPM) and the Social Security Administration (SSA).

The agreement with OPM allows Labor to disclose employee compensation benefit data so that OPM can compare the data to its records on retirees and prevent payment of concurrent benefits. The agreement with SSA is a match to ensure that dual benefits are not paid by SSA to individuals receiving employee compensation benefits.

26

How Agencies Handle Personal Information
Data Flow Modeling

Agency procedures for handling the personal information were complex. Specifically:

- The information collected was subject to numerous processes: discrete activities performed on the data from its input to the information system to the final outputs.
- A wide range of agency personnel, with various job titles, had access to some or all of the information on the forms. For example, at State, personnel with job titles such as passport specialist, adjudication manager, and consular officer had access to passport information.

27

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Data Flow Modeling (cont'd)

The following chart provides summary information on the four forms we reviewed.

Agency	Processes	Job titles
Agriculture	8	8
Education	26	9
Labor	38	4
State	39	13

28

How Agencies Handle Personal Information
Data Flow Modeling (cont'd)

In modeling the flow of personal information for each of these forms, we started at a high level, depicting the following four categories.

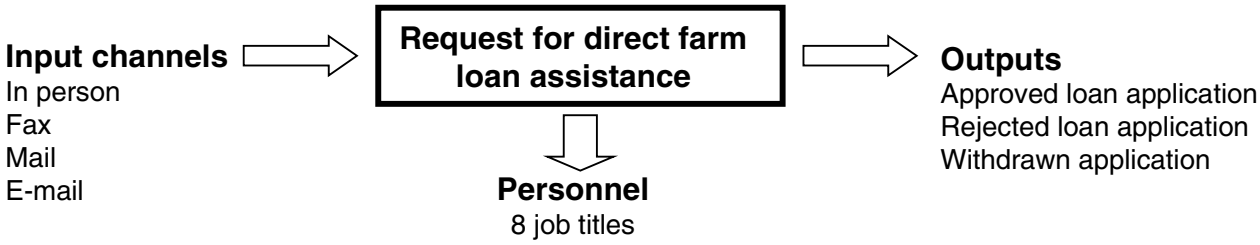
- **Input channels:** The approved methods to deliver the information to the agency.
- **Outputs:** The results or products from the processing of the information in the system.
- **Laws and guidance:** The generally applicable controls, identified by agency officials, which govern the collection, use, maintenance, and disposition of the information. They include federal law, OMB guidance, and formal agency policies and procedures.
- **Agency personnel:** The agency or contract employees having direct access to some or all of the information contained on the form. They are represented by job title, not by actual number of personnel.

We then modeled the detailed step-by-step processes for the flow of the information on the forms, from the time it was received by the agency through its disposition.

29

How Agencies Handle Personal Information
Department of Agriculture

Agriculture's Direct Loan Application overview



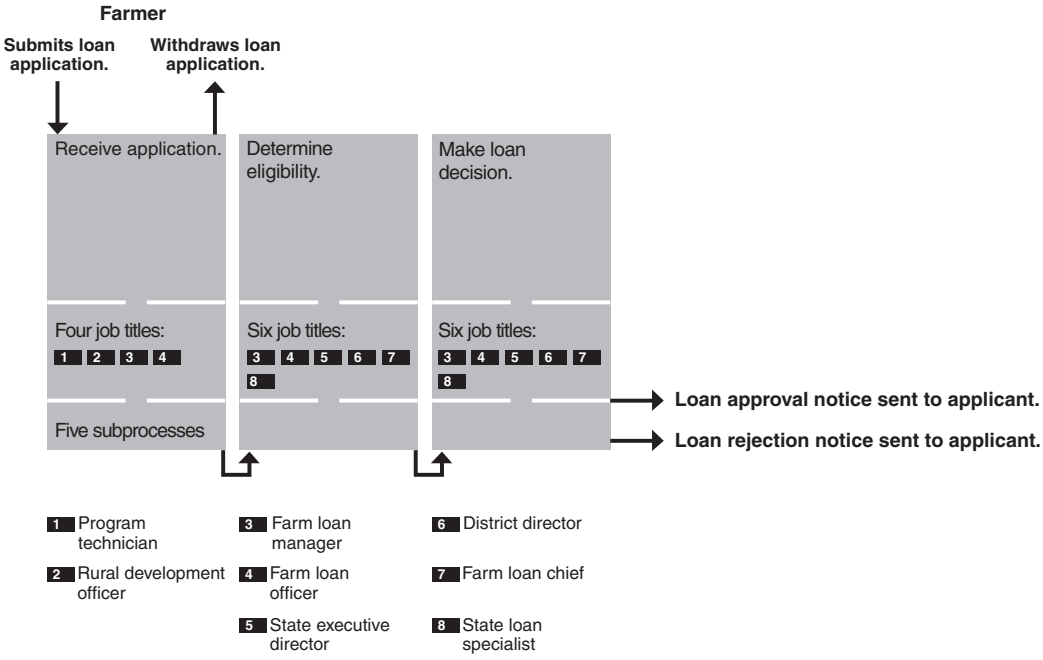
Laws & guidance: Computer Security Act; Consolidated Farm and Rural Development Act; Farm Service Agency Handbook and internal directives; Federal Records Act; Freedom of Information Act; OMB Circular A-129, Policies for Federal Credit Programs and Non-tax Receivables; other OMB guidance; Paperwork Reduction Act; Privacy Act; U.S. Code of Federal Regulations, Titles 7 and 36.

30

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Department of Agriculture

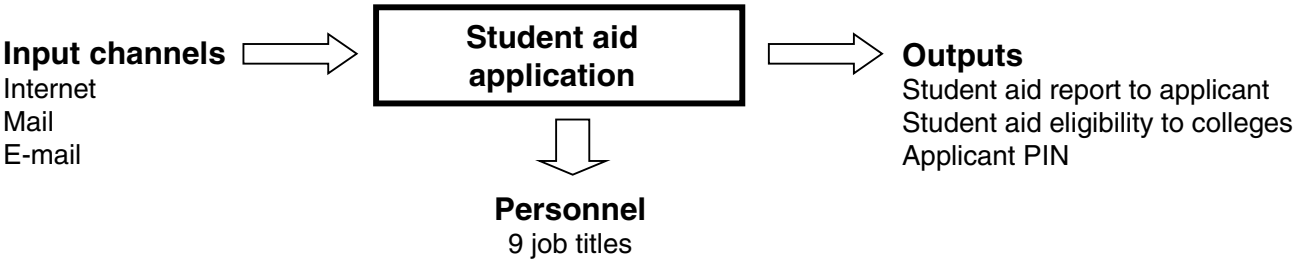
Agriculture's Direct Loan Application details



31

How Agencies Handle Personal Information
Department of Education

Education's Application for Federal Student Aid overview



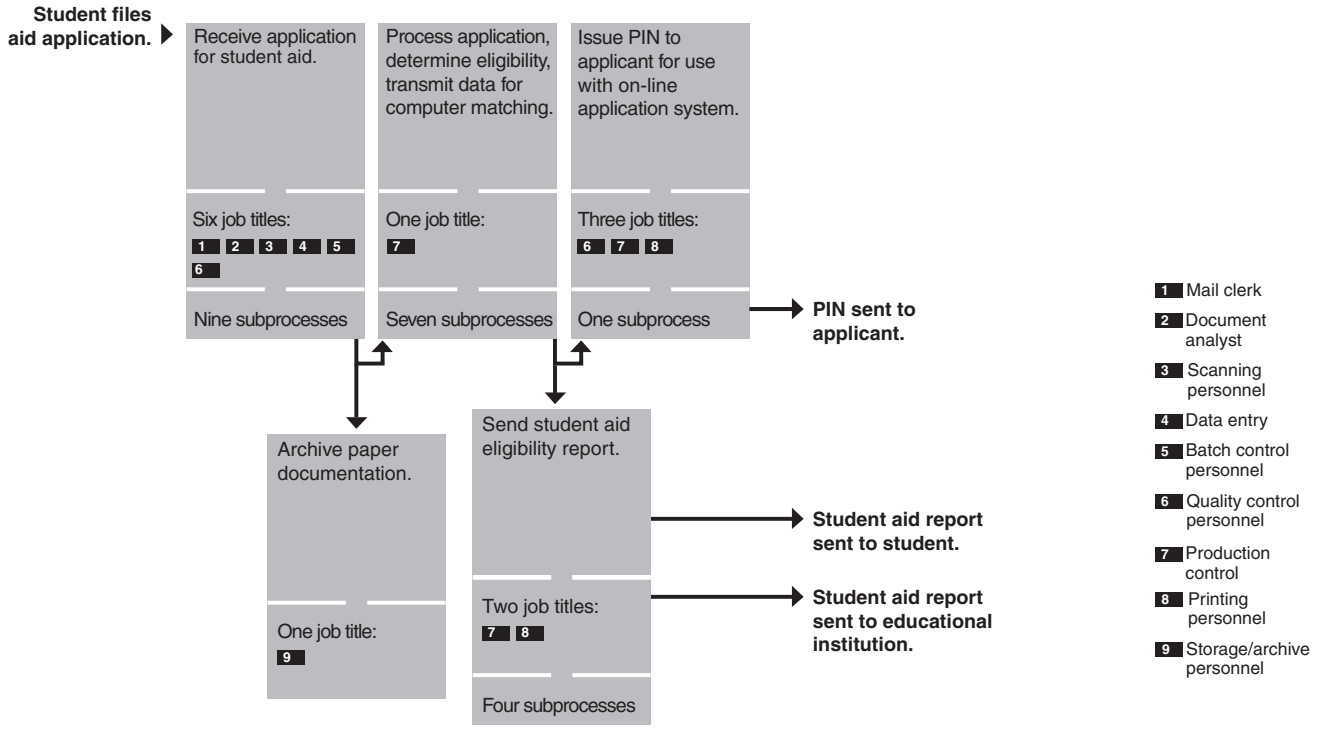
Laws & guidance: Computer Security Act; Department Central Processing System Security Plan; Office of Student Financial Assistance Guide to Information Security and Privacy; Federal Records Act; Paperwork Reduction Act; Privacy Act; Title IV Higher Education Act of 1965; U.S. Code of Federal Regulations, Title 36.

32

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Department of Education

Education's Application for Federal Student Aid details

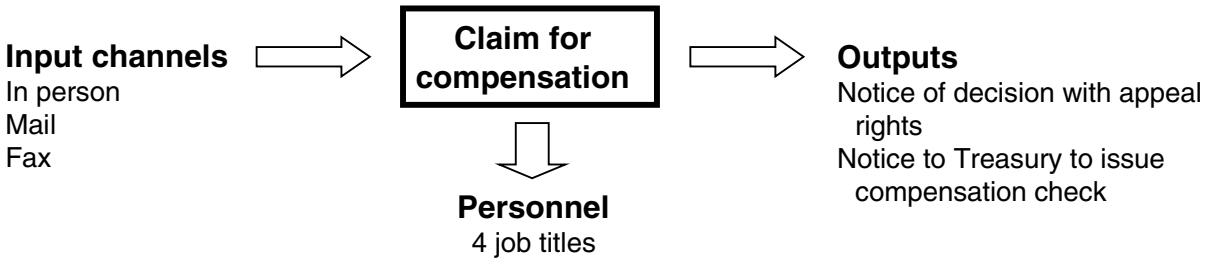


33

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Department of Labor

Labor's Claim for Federal Workers' Compensation overview



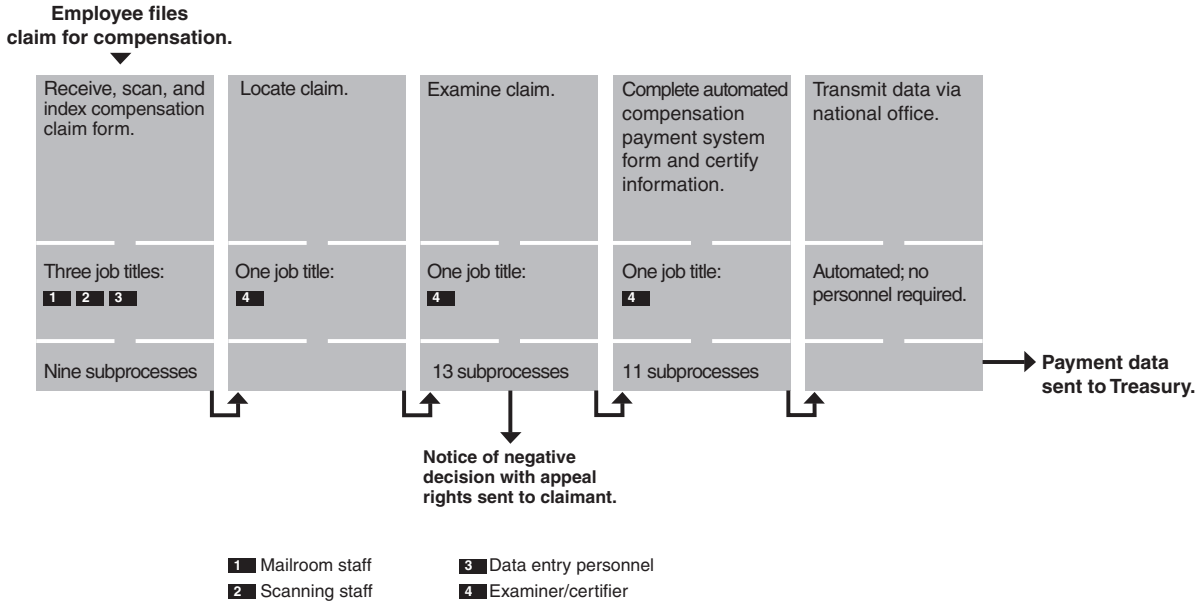
Laws & guidance: Federal Employees Compensation Act; Federal Employees Compensation Act Procedure Manual; Paperwork Reduction Act; Privacy Act; U.S. Code of Federal Regulations, Titles 20 and 36.

34

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Department of Labor

Labor's Claim for Federal Workers' Compensation details

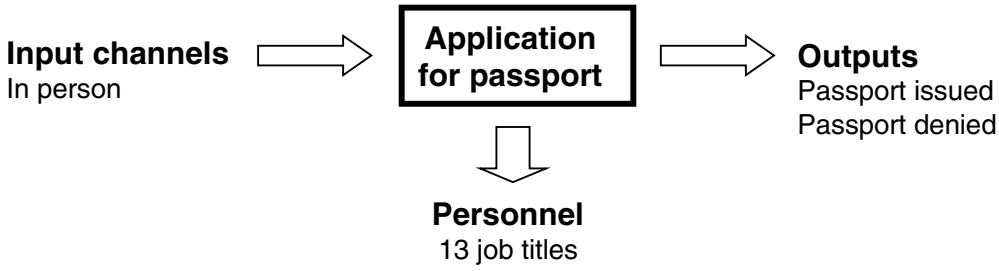


35

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Department of State

State's Passport Application overview



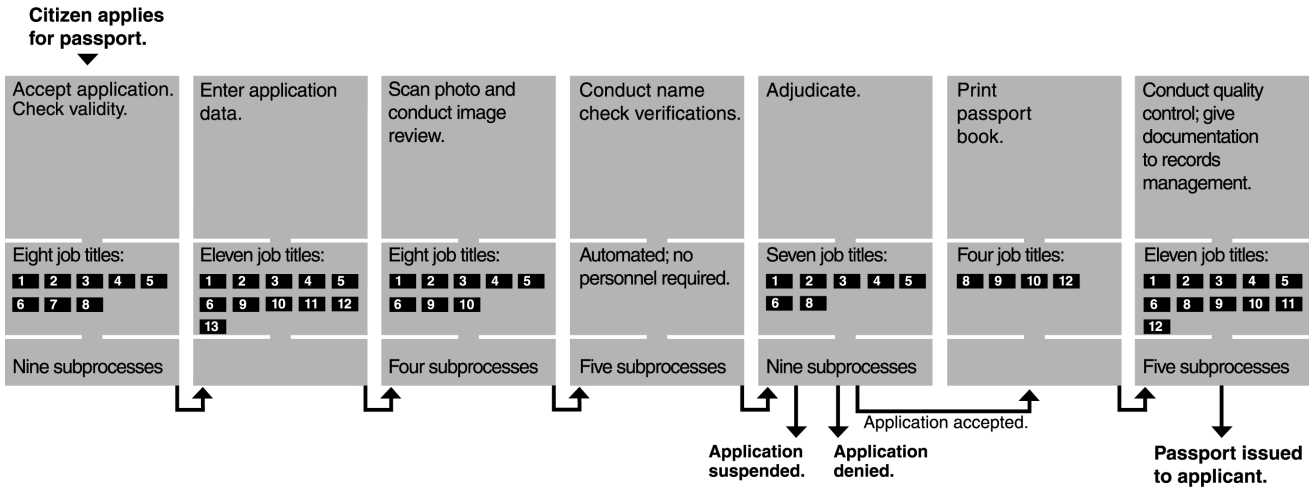
Laws & guidance: Acquisition and loss of U.S. citizenship, 8 U.S.C., Title III; Issuance and use of U.S. passports, 22 U.S.C. 211a, et seq.; Travel documentation of citizens, 8 U.S.C.; Executive Order 11295, Authority of the Secretary of State in granting and issuing U.S. passports; Code of Federal Regulations, Title 22, Parts 50, 51, 53, and Title 36; Foreign Affairs Manual, Title 7; Internal Passport Instructions; Freedom of Information Act; Government Paperwork Elimination Act; Government Performance and Results Act; Paperwork Reduction Act; Privacy Act.

36

GAO
Accountability * Integrity * Reliability

How Agencies Handle Personal Information
Department of State

State's Passport Application details



37

Agencies' Handling of Personal Information Is Generally Adequate

For the four forms, agencies were generally handling personal information adequately in key areas: information collection, privacy, security, and records management. We identified isolated instances of forms that were not accurate or current and other forms that did not contain the proper privacy notices.

The following slides provide our detailed findings in each of the four areas.

38

Agencies' Handling of Personal Information Is Generally Adequate—Collection

Under the Paperwork Reduction Act, agencies are required to follow an information review and clearance process for all forms in an information collection.

- The agency clearance process involves development of an information collection proposal meeting specific requirements, and subsequent evaluation and approval.
- After approval by the agency Chief Information Officer, OMB then assesses and can approve the form for a period of no longer than 3 years. OMB also assigns a control number and an expiration date.
- The agency must ensure that the form displays certain required information including a valid control number and a specific notice required by the PRA.
- The agency is also required to provide public notice of the proposed collection and to certify to OMB that the proposal meets PRA requirements.

39

Agencies' Handling of Personal Information Is Generally Adequate—Collection (cont'd)

In general, the agencies met the information collection requirements for these four forms. However, there were some isolated problems.

Specifically, at Labor and State, the forms displayed on the Internet showed expired OMB approvals.

In addition, Labor's electronic form did not display required PRA notices, including

- the reason for collecting the information,
- a description of how the information would be used, and
- notice of the voluntary, required, or mandatory nature of the responses.

40

Agencies' Handling of Personal Information Is Generally Adequate—Collection (cont'd)

Officials at State noted that they had submitted the clearance paperwork to OMB, which was approved after our initial meetings with State. Labor acknowledged that the form posted to the Internet was out of date and needed to be brought up to date.

Without a valid OMB number, Labor and State have no authority to obtain an individual's personal information. Further, by not having the required PRA statements on its form, Labor is not giving individuals critical information about their rights in filling out the form.

The following slides depict the results of our analysis of agency compliance with legal requirements.

41

Agencies' Handling of Personal Information Is Generally Adequate—Collection (cont'd)

Requirements	USDA	Education	Labor	State
1. The information collection proposal includes—				
need for the collection	X	X	X	X
description of the collection	X	X	X	X
plan for the collection	X	X	X	X
whether it would be covered under the Privacy Act	X	X	X	X
2. The agency collection review process ensures that—				
the need was evaluated	X	X	X	X
the proper Federal Register notice is issued	X	X	X	X
there is an inventory	X	X	X	X
there are policies and procedures to ensure each form displays the correct notices	X	X	X	X
an assessment of the burden hours was made	X	X	X	X
3. The agency clearance of proposed information collections includes—				
approval of the CIO	X	X	X	X
submission of proper material to OMB	X	X	X	X
receipt of approval for the collection and control number from OMB	X	X	X	X

Unless otherwise indicated, a check means that the condition has been met for both paper and electronic forms.

42

Agencies' Handling of Personal Information Is Generally Adequate—Collection (cont'd)

Requirements	USDA	Education	Labor	State
4. The information collection forms include proper—				
valid control numbers	X	X	No[a]	No[b]
PRA notice	X	X	No[a]	X
reasons for the collection	X	X	No	X
description of how the information will be used	X	X	No	X
time to complete the form	X	X	X	X
notice of voluntary, mandatory, or required responses	X	X	No	X
notice that a person need not respond to the form if a valid control number is missing	X	X	X	X
5. The agency provided public notice for the proposed information collection	X	X	X	X
6. The agency certified and documented that the information submitted to OMB complies with the PRA requirements	X	X	X	X

[a] While the paper forms met these requirements, the electronic versions of the form were not valid and current.
[b] State met this requirement after our evaluation was completed.

Agencies' Handling of Personal Information Is Generally Adequate—Privacy

Under the Privacy Act, an agency cannot disclose information about an individual contained in a system of records without the prior consent of the individual, unless the law authorizes the disclosure.

- When agencies collect personal information, they are required to provide a notice in the Federal Register that includes certain information, such as the name and location of the system of records, categories of individuals in the system, and routine uses of the information.
- Agencies are to have agreements for computer matching programs.
- Policies are also required for collection of personal information posted on agency Web sites.
- The forms themselves must include notice of the Privacy Act, the authority for the collection, how the information collected will be used, the applicant's rights under the Privacy Act, and the consequences to the applicant of not providing the requested information.

44

Agencies' Handling of Personal Information Is Generally Adequate—Privacy (cont'd)

The four forms we reviewed generally complied with these requirements. At Labor, however, the form posted on the Internet did not include a Privacy Act notice or the required stipulations under the Privacy Act. One agency official noted that these were on their paper version of the form, and that the electronic version needed to be updated.

Without an explicit Privacy Act notice, individuals are not made aware of their rights when providing personal information to Labor. It is left to individuals to assume that privacy rights do or do not exist, which may influence their decision to provide the information. Further, without being informed of the effect, if any, of not providing the information, individuals cannot make an informed decision about what information they want to provide.

At Agriculture, the form includes a routine use (with Labor) that is no longer valid. Forms should be updated to reflect changes in routine uses.

The following slide depicts the results of our analysis of agency compliance with privacy requirements.

45

GAO
Accountability * Integrity * Reliability

Agencies' Handling of Personal Information Is Generally Adequate—Privacy (cont'd)

Requirements	USDA	Education	Labor	State
1. The personal information is included in a Privacy Act system of records	X	X	X	X
2. Notice has been published in the Federal Register	X	X	X	X
3. The Federal Register notice includes—				
name and location of system of records	X	X	X	X
categories of individuals in the system	X	X	X	X
routine uses of the information	X	X	X	X
policies and practices regarding storage and access	X	X	X	X
title and address of official responsible for the collection	X	X	X	X
5. Computer matching agreements are in place	NA	X	X	NA
6. There are policies for collection of personal information from agency Web sites	X	X	X	X
7. Respondents are notified on the form—				
the authority of the collection and whether it is voluntary or mandatory	X	X	X[a]	X
how the information will be used	X	X	X[a]	X
possible routine uses of the information	X[b]	X	X[a]	X
consequences of not providing the information	X	X	X[a]	X

[a] While the paper forms met these requirements, the electronic versions of the form were not valid and current.
[b] The form contains a routine use that is no longer valid.

46

Agencies' Handling of Personal Information Is Generally Adequate—Security

Both the Computer Security Act and GISRA require federal agencies to provide risk-based security protections for their information systems. Agencies are required to identify their systems that contain sensitive information, and develop, maintain, and periodically review security plans for those systems. They are also required to establish an agencywide information security program that must be annually reviewed and independently evaluated. GISRA further requires that the agency Chief Information Officer be responsible for supervising information security practices at the agency.

47

Agencies' Handling of Personal Information Is Generally Adequate—Security (cont'd)

The four agencies showed evidence that these plans and programs were in existence. We did not, however, verify and assess the actual implementation of information security practices at these agencies. Further,

- GAO reports have consistently noted that information security is a high-risk area for the government in general, with potentially devastating consequences if it is not ensured.[1]
- In addition, an audit by the Agriculture Office of Inspector General (OIG) in October 2001 found physical and operational security weaknesses at some locations of the Farm Services Agency's payment and data systems.

The following slide depicts the results of our analysis of agency compliance with security requirements.

[1] U.S. General Accounting Office, *High- Risk Series: An Update*, GAO- 01- 263 (January 2001).

48

Agencies' Handling of Personal Information Is Generally Adequate—Security (cont'd)

Requirements	USDA	Education	Labor	State
1. The agency has identified systems containing sensitive information	X	X	X	X
2. The agency has an agencywide information security program	X	X	X	X
3. The agency periodically reviews its security plans as appropriate	X	X	X	X
4. The agency Chief Information Officer is responsible for information security functions in the agency	X	X	X	X[a]

[a] At State, the Bureau of Diplomatic Security shares information security responsibility.

49

Agencies' Handling of Personal Information Is Generally Adequate—Records Management

Under the Federal Records Act and implementing regulations, agencies are required to establish and maintain

- an active, continuing program for the economic and efficient management of the records of an agency; and
- policies and procedures on the use, retention, disposal, and archiving of records, as well as access to and protection of these records.

Overall, agencies were compliant with these selected records management practices. The next slide shows detailed results.

Agency officials also noted the challenges associated with managing and preserving electronic records. For example, State cited the need for additional electronic records guidance from the National Archives and Records Administration. Also, Labor recently began using a new document management system for its federal workers' compensation files. The paper applications are imaged and the electronic version becomes the permanent record copy. In our June 2002 report, *Information Management: Challenges in Managing and Preserving Electronic Records* (GAO-02-586), we discuss these challenges and make recommendations to NARA to improve electronic records management and preservation.

50

Agencies' Handling of Personal Information Is Generally Adequate—Records Management (cont'd)

The following depicts the results of our analysis of agency compliance with records management requirements.

Requirements	USDA	Education	Labor	State
1. The agency has a records management program	X	X	X	X
2. The agency has policies and procedures to govern the maintenance and use of records that include the approval of disposal schedules by NARA	X	X	X	X
3. The agency has a policy for archiving information	X	X	X	X

51

Conclusions

The collection and flow of personal information—which consists of many highly complex processes and includes substantial sharing of data with other entities—varies greatly among agencies.

For the four forms we reviewed, the agencies had policies and procedures in place concerning information collection, privacy, security, and records management. The agencies also generally followed key requirements of the Privacy Act, the Paperwork Reduction Act, and other major laws, regulations, and guidance.

However, at selected agencies there were some identified problems, such as

- keeping forms and control numbers current,
- providing adequate Paperwork Reduction Act and Privacy Act statements and notifications on forms, and
- ensuring that routine use notice statements are up to date.

52

Recommendations

To meet the requirements of the Privacy Act and other relevant laws and guidance on managing personal information, we recommend that the Secretary of Labor ensure that the appropriate agency officials review their data collection forms so that they

- are valid and up to date, and
- include the Paperwork Reduction Act and Privacy Act statements and all notices, as appropriate.

We also recommend that the Secretary of Agriculture ensure that Agriculture officials periodically assess that their routine uses for their data collections are still valid (updating the forms as appropriate).

53

Agency Comments and Our Evaluation

When commenting on a draft of this briefing, agency officials generally agreed with the facts as presented. Also, Agriculture, Education, and State officials provided technical corrections and suggestions, which were incorporated as appropriate.

54

Objectives, Scope, and Methodology

Our objectives were to

- determine how agencies are handling personal information collected on selected information collection forms; and
- evaluate the adequacy of agencies' handling of personal information against federal law, regulation, and agency guidance.

We chose one form per information collection from a system of records in each of four agencies: Department of Agriculture, Department of Education, Department of Labor, and Department of State. We chose these four agencies to reflect a broad range in the level of the paperwork burden that their information collection imposed on the public; the total paperwork burden ranged from a low of about 16.56 million hours to a high of about 186.11 million hours annually.

From these agencies, we selected four information collections that offered a range of the following variables:

- the type of information collected, e.g., demographic, financial, medical, or criminal activity;
- the collection and submission media, e.g., paper, facsimile, and/or electronic transactions;
- the type of collection, e.g., application for a direct or guaranteed loan, grant or subsidy, medical benefits and/or workplace compensation, or receipt of a service;
- the scope of the system, including computer matching agreements;
- the size of the collection burden in hours; and
- the population groups or audience using the collection, e.g., farmers, students, federal workers, and the general public.

Table 1 shows the forms that we analyzed and their owners.

Table 1: Forms Analyzed

Department	Component	Form	OMB No.
Agriculture	Farm Service Agency	"Request for Direct Loan Assistance," form FSA-410-1	0560-0167
Education	Office of Federal Student Aid	"Free Application for Federal Student Aid," form FAFSA	1845-0001
Labor	Office of Workers' Compensation Programs, Division of Federal Employees' Compensation	"Claim for Compensation," form CA-7	1215-0103
State	Bureau of Consular Affairs	"Application for U.S. Passport or Registration," form DS-11	1405-0004

Source: Agency data.

To document the flow and practices associated with the handling of personal information, we developed detailed data flows of each of these forms[4] in cooperation with agency personnel involved in the direct use of the data. First, we conducted structured interviews with top agency officials, including Chief Information Officers and staff, to understand the policy framework in place at the agency level. Second, we analyzed agency documentation on policies and procedures for using, protecting, and making available this information and mapped the procedures to the data flows. Third, we interviewed program managers responsible for the collection and use of the data collected on the forms to better understand the chosen information collection. Fourth, using data modeling software, we held in-depth data flow modeling meetings with agency staff who received, processed, maintained, and disposed of the data, as well as with the program managers responsible for the systems. Fifth, we submitted the model of the flow of personal information to the system users for their feedback to ensure the model's validity. Finally, we reviewed past GAO reports for relevant information on information collection, privacy, security, and records management.

In order to evaluate the information flows and practices against agency and federal guidance, we reviewed applicable laws and regulations and met with and obtained documentation from appropriate agency officials. We identified the key requirements of the laws and then compared these with

[4] We used a data flow modeling tool called Workflow Analyzer from Meta Software to map the flow of personal information on each form.

agency practices. Our review of laws covered the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, the Paperwork Reduction Act of 1995, the Government Paperwork Elimination Act of 1998, the Computer Security Act of 1987, the Government Information Security Reform Act of 2000, the Federal Records Act, and the Code of Federal Regulations. We also reviewed pertinent OMB guidance.

We conducted our review from March 2001 to July 2002, in accordance with generally accepted government auditing standards.

Selected Bibliography

General

Internal Revenue Service Technical Manual, Office of Privacy Advocate. *Privacy Impact Assessment.* Version 1.3. Washington, D.C.: December 17, 1996.

Office of Management and Budget. *FY 2001 Report to Congress on Federal Government Information Security Reform.* Washington, D.C.: February 13, 2002.

Office of Management and Budget, *OIRA. Managing Information Collection and Dissemination: Fiscal Year 2002.* Washington, D.C.: n.d.

Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information.* Washington, D.C.: June 6, 1995.

SRA International, Inc. *Report on Current Recordkeeping Practices within the Federal Government.* Prepared for the National Archives and Records Administration. Arlington, VA: December 10, 2001.

Agriculture

Department of Agriculture, Office of Inspector General, Great Plains Region. *Farm Service Agency/Commodity Credit Corporation: Security Over Information Technology Resources.* 03099-47-KC. Washington, D.C.: October 31, 2001.

Education

Department of Education, Office of Inspector General, *Final Audit Report on Audit of the Department's Records Management Program.* ED-OIG/A11-A0011. Washington, D.C.: September 2001.

Related GAO Products

General

Paperwork Reduction Act: Changes Needed to Annual Report. GAO-02-651R. Washington, D.C.: April 29, 2002.

Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected. GAO-02-691T. Washington, D.C.: April 29, 2002.

Paperwork Reduction Act: Burden Increases and Violations Persist. GAO-02-598T. Washington, D.C.: April 11, 2002.

Information Resources Management: Comprehensive Strategic Plan Needed to Address Mounting Challenges. GAO-02-292. Washington, D.C.: February 22, 2002.

U.S. Postal Service: Update on E-Commerce Activities and Privacy Protections. GAO-02-79. Washington, D.C.: December 21, 2001.

Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-02-231T. Washington, D.C.: November 9, 2001.

Electronic Government: Challenges Must Be Addressed With Effective Leadership and Management. GAO-01-959T. Washington, D.C.: July 11, 2001.

Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information. GAO-01-126SP. Washington, D.C.: April 1, 2001.

Information Management: Progress in Implementing the 1996 Electronic Freedom of Information Act Amendments. GAO-01-378. Washington, D.C.: March 16, 2001.

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. GAO-01-277. Washington, D.C.: February 26, 2001.

High-Risk Series: An Update. GAO-01-263. Washington, D.C.: January 1, 2001.

Electronic Government: Government Paperwork Elimination Act Presents Challenges for Agencies. GAO/AIMD-00-282. Washington, D.C.: September 15, 2000.

Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles. GAO/AIMD-00-296R. Washington, D.C.: September 11, 2000.

Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy. GAO/GGD-00-191. Washington, D.C.: September 5, 2000.

Electronic Government: Federal Initiatives Are Evolving Rapidly But They Face Significant Challenges. GAO/T-AIMD/GGD-00-179. Washington, D.C.: May 22, 2000.

Information Technology: Comments on Proposed OMB Guidance for Implementing the Government Paperwork Elimination Act. GAO/AIMD-99-228R. Washington, D.C.: July 2, 1999.

Corps of Engineers Electronic Signature System. GAO/AIMD-97-18R. Washington, D.C.: November 19, 1996.

Agriculture

Farm Loan Programs: Improvements in the Loan Portfolio but Continued Monitoring Needed. GAO-01-732T. Washington, D.C.: May 16, 2001.

USDA Electronic Filing: Progress Made, But Central Leadership and Comprehensive Implementation Plan Needed. GAO-01-324. Washington, D.C.: February 28, 2001.

Information Security: USDA Needs to Implement Its Departmentwide Information Security Plan. GAO/AIMD-00-217. Washington, D.C.: August 10, 2000.

Information Security: Software Change Controls at the Department of Agriculture. GAO/AIMD-00-186R. Washington, D.C.: June 30, 2000.

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-99-227. Washington, D.C.: July 30, 1999.

Education

Student Financial Aid: Use of Middleware for Systems Integration Holds Promise. GAO-02-7. Washington, D.C.: November 30, 2001.

Education Information Security: Improvements Made But Control Weaknesses Remain. GAO-01-1067. Washington, D.C.: September 12, 2001.

Financial Management: Internal Control Weaknesses Leave Department of Education Vulnerable to Improper Payments. GAO-01-585T. Washington, D.C.: April 3, 2001.

Major Management Challenges and Program Risks: Department of Education. GAO-01-245. Washington, D.C.: January 1, 2001.

Student Loans: Improvements in the Direct Loan Consolidation Process. GAO/HEHS-99-19R. Washington, D.C.: November 10, 1998.

Labor

Office of Workers' Compensation Programs: Further Actions Are Needed to Improve Claims Review. GAO-02-637. Washington, D.C.: May 9, 2002.

Office of Workers' Compensation Programs: Further Actions Are Needed to Improve Claims Review. GAO-02-725T. Washington, D.C.: May 9, 2002.

Department of Labor: Status of Achieving Key Outcomes and Addressing Major Management Challenges. GAO-01-779. Washington, D.C.: June 15, 2001.

Workers' Compensation: Action Needed to Reduce Payment Errors in SSA Disability and Other Programs. GAO-01-367. Washington, D.C.: May 4, 2001.

Office of Workers' Compensation Programs: Goals and Monitoring Are Needed to Further Improve Customer Communications. GAO-01-72T. Washington, D.C.: October 3, 2000.

Information Security: Software Change Controls at the Department of Labor. GAO/AIMD-00-192R. Washington, D.C.: June 30, 2000.

Major Management Challenges and Program Risks: Department of Labor. GAO/OCG-99-11 Washington, D.C.: January 1, 1999.

Federal Employees' Compensation Act: Percentages of Take-Home Pay Replaced by Compensation Benefits. GAO/GGD-98-174. Washington, D.C.: August 17, 1998.

State

Electronic Signature: Sanction of the Department of State's System. GAO/AIMD-00-227R. Washington, D.C.: July 10, 2000.

Information Security: Software Change Controls at the Department of State. GAO/AIMD-00-199R. Washington, D.C.: June 30, 2000.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00