

For: FSA Employees and Contract Employees

Management of Sensitive (Privacy Act Protected) Data

Approved by: Deputy Administrator, Management



1 Overview

A Background

A massive security breach disclosed last month at another government agency has triggered sweeping reviews of information security policies. A laptop personal computer (PC) and external hard drive were stolen from a data analyst’s home. This potentially compromised the names, dates of birth, Social Security numbers, and some disability ratings for up to 26.5 million U.S. veterans and some spouses, personal information on as many as 1.1 million military members on active duty, 430,000 members of the National Guard, and 645,000 members of the Reserve.

Congress is deeply concerned that the government failed to safeguard this data that in the wrong hands could be used for identity theft, credit card fraud, and other crimes.

Earlier this month, officials at the OMB and the Government Accountability Office stated that federal agencies as a whole need to review their processes for collecting, storing, and controlling access to data.

USDA recently announced that an unauthorized third party accessed a USDA computer system affecting Washington, DC-based employees and contractors. The system included a database containing employee names, Social Security numbers, and photos. Approximately 26,000 current and former Washington, DC-based USDA employees and contractors are potentially affected. It is unknown whether personal information was viewed by unauthorized persons.

All employees and contract employees have a significant responsibility to ensure that:

- sensitive data entrusted to them is secure
- both FSA’s customer’s and employee’s sensitive personal data is not divulged to unauthorized personnel, lost, or stolen.

Disposal Date	Distribution
October 1, 2007	All FSA employees and contractors; State Offices relay to County Offices

Notice IRM-371

1 Overview (Continued)

B Purpose

This notice provides policy for managing Privacy Act protected data to help safeguard the information. All FSA employees, contract employees, and partners who handle Privacy Act protected data in the performance of their duties must comply with this and all other applicable Federal, USDA, FSA, and OCIO ITS requirements.

C Sources of Authority

The sources of authority are:

- the Privacy Act of 1974, as amended (Pub. L. 93-579, 5 U.S.C. 552a)
- 6-IRM
- Notice IRM-368
- Notice AS-2100
- the memorandum for all USDA employees and contractors from the CIO about “Protecting and Safeguarding Privacy Act Protected Information,” dated June 16, 2006 (see Exhibit 1)
- USDA Cyber Security Manual Series 3500 and associated Cyber Security guidance, especially:
 - USDA Departmental Manual (DM) 3505-000, USDA Computer Incident Response Procedures Manual (March 20, 2006)
 - DM 3530-005, Encryption Security Standards (February 17, 2005)
 - DM 3550-002, Sensitive But Unclassified (SBU) Information (February 17, 2005)
- USDA Administrative Bulletin Departmental Regulation (DR) 3602-001, OCIO-ITS Security Policy Manual
- ITS 8000-001, Incident Reporting, Handling, and Response Security Procedures Guide
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 197, Advanced Encryption Standard.

2 Policy

A Responsibility

It is the responsibility of each individual with access to Privacy Act protected data to:

- use Privacy Act protected data in an appropriate manner
- comply with all applicable Federal laws, NIST guidance, and USDA, FSA, and ITS regulations
- safeguard Privacy Act protected data.

B Definition of Privacy Act Protected Data

Privacy Act protected data is defined as any data that contains personal identifying information including a personal name and any of the following:

- Social Security number
- date of birth
- home address
- financial information
- other items, collections, or groupings of information about an individual such as education (excluding training information for government employees), medical history, and criminal or employment history that contains a personal name or identifying number, symbol, or other identifying particular assigned to the individual.

While formal Government Systems of Records comprise most of the Privacy Act protected data used by FSA, any records or data that meet the above criteria can have privacy implications and should be protected accordingly.

2 Policy (Continued)

C Restrictions on Downloading and Storage of Privacy Act Protected Data

No Privacy Act protected data is to be downloaded to, or stored on, any of the following outside of a properly secured government building or approved facility without prior approval of the FSA CIO; see subparagraph 4 A for contact information:

Notes: This prohibition applies to both government-owned and personally-owned equipment.

Approved facilities can include sites used to store data backups, sites used for disaster recovery, and approved contractor facilities.

No hard copies shall be stored outside of a properly secured government building or approved facility without prior approval of the FSA CIO.

- home PC's and portable computers, including laptops, notebooks, and tablet computers
- portable electronic devices, including Personal Data Assistants, text messaging devices (including Blackberries), cell phones, digital cameras, Apple iPods, scanners, and other mobile devices that can receive, store, or transmit data
- hard disk drives, including both internal and external hard drives
- removable media, including tapes, portable disk drives, Zip drives, Universal Serial Bus flash drives (data/memory sticks or thumb drives), smart cards, compact disks (CD-R, CD-ROM, CD-RW, etc.), DVD's (DVD-R, DVD+R, DVD-RAM, DVD-ROM, DVD-RW, DVD+RW, etc.), and diskettes ("floppy" disks).

D Restrictions on the Transmission of Privacy Act Protected Data

If it is necessary to transfer any Privacy Act protected data outside of a properly secured government building or approved facility, the data needs to be protected.

Privacy Act protected data (Pub. L. 93-579):

- may be transmitted across a LAN if the LAN is accredited; USDA LAN's are accredited
- **shall not** be transmitted over the Internet or e-mail systems unless encrypted through an approved method.

Note: Users should contact ITSD for information on methods, including encryption, to ensure the safety and security of the Privacy Act protected data while it is in transit, unless procedures to secure the data have already been agreed upon with ITSD or OCIO.

2 Policy (Continued)

D Restrictions on the Transmission of Privacy Act Protected Data (Continued)

For more information on protecting Privacy Act Protected data during transfer or transmission, or on encryption, contact the ITSD Information Security Office help desk, by:

- e-mail to security@kcc.usda.gov
- telephone at 816-926-6537.

E Reporting Disclosure or Misuse of Privacy Act Protected Data

Any accidental or deliberate disclosure or suspected misuse of Privacy Act protected data should be reported immediately to the appropriate authorities.

All users shall notify their immediate supervisor, management officials, and their local Security Liaison Representatives (SLR) if they suspect a Privacy Act protected data incident. The identity of the person reporting an incident or violation shall be kept confidential and released only on a need-to-know basis. The immediate supervisor, management officials, and local SLR shall notify the State SLR or Information Security Officer, who will follow proper computer security incident reporting procedures.

F Disciplinary Action for Deliberate Disclosure or Misuse of Privacy Act Protected Data

Any person who willfully violates Federal laws or USDA, FSA, or applicable ITS policies is subject to disciplinary action, including suspension or dismissal.

The Privacy Act states that: “Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information... and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.”

Notice IRM-371

3 Training Available Through AgLearn

A AgLearn Class, “USDA Privacy Basics”

The USDA Privacy Basics course:

- introduces the Privacy Act of 1974 and how Privacy Act information is handled and secured at USDA
- teaches how protecting Privacy Act protected data relates to our work at USDA.

Note: Detailed information on accessing this class can be found in Notice IRM-368.

B Information for FSA Employees

All FSA employees working with Privacy Act protected data are encouraged to take this AgLearn class that was referred to Exhibit 1 from USDA’s CIO. Per Notice IRM-368, this class is mandatory for SLR’s.

C Information for FSA Contractors

FSA contractors working with Privacy Act protected data must obtain approval from their Contracting Officer Representative or Contracting Officer Technical Representative if they want to take this class. Information on obtaining AgLearn licenses for contractors can be found in Notice IRM-370.

4 Contacts

A Contacts for This Notice

Direct any questions about this notice to either of the following:

- Brian Davies, FSA ISSPM, by:
 - e-mail to brian.davies@wdc.usda.gov
 - telephone at 202-720-2419.
- Steven Sanders, FSA CIO, by:
 - e-mail to steve.sanders@wdc.usda.gov
 - telephone at 202-720-5320.

Notice IRM-371

4 Contacts (Continued)

B Contacts for Privacy Act of 1974, as Amended (Pub. L. 93-579, 5 U.S.C. 552a)

Direct any questions about the Privacy Act to either of the following:

- Norma Ferguson, FSA Privacy Act Officer, by:
 - e-mail to **norma.ferguson@wdc.usda.gov**
 - telephone at 202-720-5534

- Wilbur Crawley, USDA OCIO Cyber Security, by:
 - e-mail to **wilbur.crawley@usda.gov**
 - telephone at 301-504-4154.

C Contacts for AgLearn

The following table provides contacts for guidance or assistance with AgLearn.

IF...	THEN...
employee in any office	<ul style="list-style-type: none"> • click “Help” on any of the AgLearn pages • click “Contact Us” for FSA contact information • call the AgLearn help desk at 866-633-9394.
National Office contract employee	contact Bessy Plaza, HRD, National Office training coordinator, by: <ul style="list-style-type: none"> • e-mail to bessy.plaza@wdc.usda.gov • telephone at 202-401-0365.
employee in: <ul style="list-style-type: none"> • State Office • Kansas City • St. Louis • APFO 	contact Ruby Hervey, KCHRO, training coordinator, by: <ul style="list-style-type: none"> • e-mail to ruby.hervey@kcc.usda.gov • telephone at 816-926-2834.

Memorandum for All USDA Employees and Contractors

The following is from the CIO about Protecting and Safeguarding Privacy Act Protected Information, dated June 16, 2006.

	JUN 16 2006
United States Department of Agriculture	
Office of the Chief Information Officer	MEMORANDUM FOR ALL USDA EMPLOYEES & CONTRACTORS
1400 Independence Avenue SW	FROM: David M. Combs Chief Information Officer <i>David M. Combs</i>
Washington, DC 20250	SUBJECT: Protecting and Safeguarding Privacy Act Protected Information

Several compromises of Privacy Act protected information have occurred at other federal departments over the last several weeks. I want to remind USDA employees, contractors and partners of their responsibility to ensure that the personal information held by their agencies on customers and employees is safeguarded and used only for the purposes for which it has been collected.

The Privacy Act of 1974, as amended (5 USC 552a) states that:

Each agency that shall collect and maintain only information about an individual as is relevant and necessary to accomplish its mission.

No agency shall disclose any record which is contained in a system of records...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains except to those officers and employees who have a need for the record in the performance of their duties.

Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information ... and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

The Department of Agriculture has established administrative, technical and physical safeguards to comply with the Privacy Act as well as protect its information technology systems. A web-based training course entitled "OCIO Privacy Basics" is available on AgLearn.

All USDA employees, contractors and partners who handle Privacy Act protected data in the performance of their duties must comply with all Department requirements. If you have any questions, please contact Wilbur Crawley at 301-504-4154 or email him at Wilbur.Crawley@usda.gov.

AN EQUAL OPPORTUNITY EMPLOYER