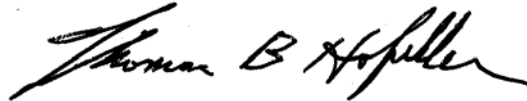


For: FFAS Employees

Safeguarding Employee Personally Identifiable Information (PII)

Approved by: Acting Administrator



1 Overview

A Background

OPM is requiring agencies to implement guidance for safeguarding employee PII, consistent with recommendations formulated by the President’s Identity Theft Task Force.

The intent is to minimize Federal employee identify theft and fraud by:

- eliminating using SSN’s as identifiers
- strengthening the protection of PII, including SSN’s, from theft or loss.

HRD is collecting, reviewing, and analyzing forms, reports, and systems that are used to conduct business and exploring alternatives that can be used to protect PII.

B Purpose

This notice provides:

- information about PII
- guidance on protecting employee PII when conducting business with HRD.

C Contacts

If there are questions about this notice, contact either of the following HRD employees:

- Juliet McBride, Employee Programs Branch, 202-401-0683, TTY 202-205-9057
- Rande Young, Special Projects and Information Management Branch, 202-401-0267, TTY 202-205-9057.

Disposal Date	Distribution
February 1, 2008	All FSA, RMA, and FAS offices. State Offices relay to County Offices

Notice PM-2624

1 Overview (Continued)

D Authorities and References

Guidelines referenced in this notice are according to the following documents:

- Notice AS-2137
- OCIO Memorandum, "Definition and Controls over PII 'Cuff' Systems," dated July 23, 2007
- OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology," dated July 12, 2006
- OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007
- OPM Memorandum, "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identify Theft," dated June 18, 2007 (see Exhibit 1)
- Privacy Act of 1974.

2 PII

A Definition of PII

PII means any information about an individual that is maintained by an agency that includes, but is not limited to, financial transactions, medical or criminal history, and information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc, including any other personal information that is linked or linkable to an individual.

B Documents, Forms, Reports, and Systems Containing PII

PII is:

- commonly found on human resource (HR) documents, forms, reports, and systems that are maintained and used when communicating with clients

Examples: Forms such as AD-287-2, AD-658P, AD-717, CA-1, CA-2, FAS-10, FFAS-10, FFAS-956, FSA-358, FSA-958, OGE-450, SF-182, SF-278, SF-2809, SF-2817, SF-52, and TSP-1 and NFC reports such as staffing and focus.

- communicated in systems such as Employee Personnel Page, EmpowHR, Federal Retirement Benefit Web, OWCP Agency Query System, and the Star Web.

Notice PM-2624

3 Guidelines for Protecting Employee PII

A Safeguarding Employee PII

All employees shall follow this notice and OPM guidelines (see Exhibit 1) in an effort to safeguard employee PII on HR documents and systems.

B Additional Measures for Protecting Employee PII

Individuals who provide, receive, review, or process HR related information (such as documents, reports, and forms) and use systems to convey sensitive information should take the following measures to protect employee privacy:

- hand carry or send by courier, documents containing PII ; do **not** overstuff envelopes to avoid exposure of PII
- see Notice AS-2137 for requirements and methods for shipping PII through both internal and external physical transportations systems
- if FAXing, notify the recipient **before** FAXing and ask the recipient to call and verify FAX receipt
- shred **all** waste documents containing PII; see subparagraph 2 A for definition of PII
- ensure that all documents, forms, and reports containing PII are safeguarded at **all** times
- lock-up all documents containing PII at the end of each workday
- do **not** send e-mail messages that contain PII unless encrypted.

4 Action

A Employee Action

All employees shall follow this notice and OPM guidelines (see Exhibit 1).

B Manager and Supervisor Action

Managers and supervisors shall ensure that employee PII is safeguarded at all times in an effort to prevent identify theft and fraud.

C FSA State Administrative Officer Action

FSA State Administrative Officers shall ensure that employees adhere to guidelines in Notice IRM-400 when removing employees from HR system access.

OPM Memorandum, “Guidance on Protecting Federal Employee Social Security Numbers and Combating Identify Theft”

All employees shall follow OPM’s guidelines in this memorandum and attachment in an effort to protect employee PII on HR documents and systems.



The Director

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

June 18, 2007

MEMORANDUM FOR CHIEF HUMAN CAPITAL OFFICERS

FROM: LINDA M. SPRINGER
DIRECTOR 

SUBJECT: Guidance on Protecting Federal Employee Social Security Numbers and Combating Identify Theft

The Office of Personnel Management (OPM) is issuing guidance to help agencies achieve a consistent and effective policy for safeguarding the Social Security Numbers (SSNs) of Federal employees. The intent of this guidance is to minimize the risk of identity theft and fraud in two ways: (1) by eliminating the unnecessary use of SSN as an identifier, and (2) by strengthening the protection of personal information, including SSNs, from theft or loss. We are also studying the advisability of issuing regulations to enforce this guidance. The new guidance is consistent with recommendations that have been formulated by the President’s Identity Theft Task Force.

Applying this guidance is a first step in protecting the personal identity of Federal employees. Efforts are also underway to develop requirements for a new Government-wide employee identifier which will replace the Social Security Number as an employee identifier. Once this new employee identifier is established, it will be an important tool in combating the serious and growing problem of identity theft.

Each agency should maintain security policies that, at a minimum, contain the content or reference the requirements presented in this document. The attachment included with this document identifies and highlights existing regulatory requirements, as well as specific measures we are urging agencies to implement as soon as possible, if they have not already done so. For a more complete listing of the regulatory requirements relevant to maintaining personnel records, please refer to 5 CFR part 293.

If you have any questions or need additional information, please contact your OPM Human Capital Officer. Thanks for your continued support in protecting and safeguarding our employees’ sensitive and personal information.

Attachment:
“Protecting Employee Personal Identifiers and Combating Identity Theft”

cc: Human Resources Directors

OPM Memorandum, “Guidance on Protecting Federal Employee Social Security Numbers and Combating Identify Theft” (Continued)**Protecting Employee Personal Identifiers
And Combating Identity Theft****All agencies should be aware of the following regulatory requirements that are currently in effect:**

- 5 CFR 293.103 - The head of each agency shall ensure that persons having access to or involved in the creation, development, processing, use, or maintenance of personnel records are informed of pertinent recordkeeping regulations and requirements of the Office of Personnel Management and the agency.
- 5 CFR 293.105(b)(1) - Agencies may not require individuals to disclose their Social Security Number (SSN) unless disclosure would be required under--
 - Federal statute; or
 - any statute, Executive order, or regulation that authorizes any Federal, State, or local agency maintaining a system of records that was in existence and operating prior to January 1, 1975, to request the SSN as a necessary means of verifying the identity of an individual.
- 5 CFR 293.105(b)(2) - Individuals asked to voluntarily provide their SSN shall suffer no penalty or denial of benefits for refusing to provide it.
- 5 CFR 293.106 – Agencies shall establish administrative, technical, and physical controls to protect information in personnel records from unauthorized access, use, modification, destruction, or disclosure.
- 5 CFR 293.107 – Managers of automated personnel records shall establish administrative, technical, physical, and security safeguards for data about individuals in automated records, including input and output documents, reports, punched cards, magnetic tapes, disks, and on-line computer storage.
- 5 CFR 293.108 – Agencies shall require all employees responsible for the creation, development, maintenance, processing, use, dissemination, and safeguarding of personnel records to be familiar with the rules of conduct presented in this section.
- 5 CFR 1001.102 – Agencies must ensure that all employees and contractors are reminded of their obligation to follow the Privacy Act.

In addition, agencies should ensure that the following measures, if not already in place, are implemented as soon as possible:

- If Social Security Numbers are collected, they should be collected at the time of an employee’s appointment and entered into the human resources and payroll systems. The collection tool (if paper-based) should be stored in a secure location until it is no longer required. Disposal of all paper-based collection tools (i.e., forms, letters, and other correspondence) must be in accordance with the General Record Schedule issued by the National Archives and Records Administration.
- Unnecessary printing and displaying of the SSN on forms, reports, and computer display screens should be eliminated.
- Access to the SSN should be restricted to only those individuals whose official duty requires such access. A listing of all access authorizations should be maintained and monitored regularly for continued applicability.

OPM Memorandum, “Guidance on Protecting Federal Employee Social Security Numbers and Combating Identify Theft” (Continued)

- Those individuals who are authorized to access the SSN must understand their responsibility to protect sensitive and personal information. This includes securing this information when working from home or another remote location. Annual training and educational programs, which include Privacy Act and Freedom of Information Act requirements, should be employed to reinforce awareness of these responsibilities.
- Privacy and confidentiality statements that describe accountability clearly and warn of possible disciplinary action for unauthorized release of the Social Security Number and other personally identifiable information should be signed by all individuals who have access to the Social Security Number.
- Agency telework policies and written agreements must be in compliance with Federal privacy protection policies, including policies governing the protection of employee Social Security Numbers.
- Supervisory approval should be required before an authorized individual can access, transport, or transmit information or equipment containing Social Security Numbers outside agency facilities.
- Electronic records containing Social Security Numbers should be transported or transmitted in an encrypted or protected format as prescribed in current OMB guidance regarding the protection of sensitive agency information.
- Paper-based records containing Social Security Numbers should be transported in wheeled containers, portfolios, briefcases, or similar devices that are locked when the records are not in use. These containers should be identifiable by tag, label, or decal with contact and mailing information.
- Required access to Social Security Numbers, including data entry, printing, and screen displays must be conducted in a secure location to protect against unauthorized exposures.
- All security incidents involving personally identifiable information, especially SSN(s), must be reported in accordance with current OMB guidance regarding the reporting of incidents involving personally identifiable information. In addition, all individuals authorized to access the Social Security Numbers must be familiar with their incident reporting requirements.
- All disclosures of information containing Social Security Numbers and other personally identifiable data must be made in accordance with established regulations and procedures.
- Written procedures describing the proper labeling, storage, and disposal of printed material containing Social Security Numbers and other personally identifiable data must be established and communicated to employees.
- When the Social Security Number is required as a data entry parameter, it must not be displayed on the input screen except when establishing the initial human resources or payroll record. In all other record retrieval and access authorization processes, the Social Security Number must be masked with asterisks or other special characters, similar to the technique used when handling passwords and PINs.
- Adequate internal control procedures must be employed to ensure the proper monitoring of authorized and unauthorized access to Social Security Numbers and other personally identifiable information.