



APR 18 2011

United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

TO: Agency Administrators
Agency Deputy Administrators for Management
Departmental Management
Agency Chief Information Officers
Information Systems Security Program Managers

FROM: Charles T. McClam
Deputy Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Minimum Safeguards for Protecting Personally Identifiable Information

USDA in the fulfillment of its mission collects, maintains, and processes vast amounts of sensitive and personally identifiable information (PII). As such, each USDA employee, contractor, affiliate, and partner has a vital role in protecting all personally identifiable and sensitive information entrusted to them. All USDA employees, contractors, partners and affiliates must exercise extreme care in the handling of PII. Failure to properly protect and control PII may result in disciplinary actions, in accordance with USDA policies.

The Office of Management and Budget (OMB) established guidance for protecting PII in memoranda M-06-15, "*Safeguarding Personally Identifiable Information*" and M-06-16, "*Protection of Sensitive Agency Information*." In these memos, the OMB defines PII as "any combination of information about an individual maintained by the agency, including but not limited to name, social security number, date of birth, maiden name, biometric record number, home address, education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity."

In addition to OMB's memoranda, the Office of the Chief Information Officer (OCIO) issued multiple memoranda on protecting and safeguarding paper based, and electronic PII. USDA employee, contractors, affiliates, and partners are reminded that the removal PII (either paper based or electronic) from the workplace without prior written authorization from the USDA unit manager or other authorized senior agency official is prohibited.

Paper based PII

Paper-based PII incidents can be reduced by securing all PII in an approved locked storage container or device when not in use, and adhering to the Department's physical transport of PII guidance (attached).

Mobile Media Storage Devices

Extreme care must be exercised in the storage, transport, and usage of mobile media devices containing PII. Mobile media devices include, but are not limited to; compact disk (CD), digital video device (DVD) and universal serial bus (USB).

Individuals who use CDs and DVDs to process PII, must encrypt and password protect the file containing the PII, and transport the media device and the password separately. USB devices used by USDA employees, contractors, and affiliates to process or store PII must be Government issued encrypted USBs devices. The processing and storage of PII and sensitive information on a personal and/or unencrypted USB is strictly prohibited.

Password Protection

Use a complex password for files containing PII which are being stored or transmitted. The password complexity should contain upper and lower case letters, numbers, and special character. The password should be transmitted separately from the file.

Reporting a PII Incident

Immediately report PII incidents to the PII hot line at 1-877-PII-2-YOU, or 1-877-744-2968. The hotline is operational twenty-four hours a day seven days a week.

PII Requirements Assistance

USDA employees, contractors, and affiliates should consult their agency Information Systems Security Program Manager, Agency Privacy Official, or agency Chief Information Security Officer for assistance in satisfying the above requirements.

If you have any questions regarding this memorandum, please contact Ms. Ray Payton, Chief Privacy Officer at (202) 720-8755 or ray.payton@ocio.usda.gov.

Attachment

Personally Identifiable Information (PII) Physical Transport – Double Wrap Procedures

Personal Identifiable Information (PII) Physical Transport—Double Wrap Procedures

Instructions:

USDA processes all types of sensitive information and it is essential that this information be properly handled and protected. PII is considered Sensitive But Unclassified (SBU) Information. Careless handling and transporting PII information puts USDA at risk.

USDA policy prescribes specific procedures for the transport of PII. When Physical Transport is necessary:

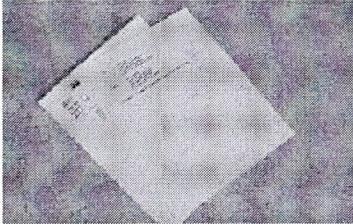
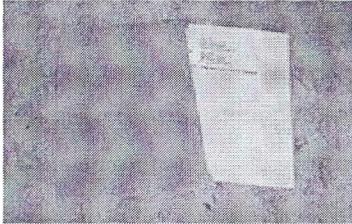
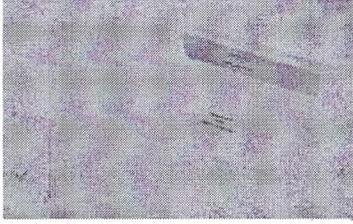
1. Encrypt portable media containing PII
2. Use NIST approved encryption method
3. Double wrap portable media
4. Transport by Postal Service or another authorized delivery service
5. Transmit decryption key separately via certified mail
6. Mark physical documents containing PII: "Sensitive But Unclassified / Sensitive Security Information—Disseminate on a Need-to-Know Basis Only"
7. Documents should be double wrapped
8. Transport by Postal Service or another authorized delivery service

Portable media should be double-wrapped in an opaque package or container that is sealed sufficiently to prevent inadvertent opening and to show signs of tampering. The package must be sent via a certified carrier with an ability to track pickup, receipt, transfer, and delivery.

Portable media may be transmitted by interoffice mail or briefcase provided it is double-wrapped to afford sufficient protection against inadvertent or unauthorized access.

Please follow the instructions below when transporting PII information. The steps listed on the chart, must be followed with no exceptions. If you have any questions or concerns, please contact us at cyber.incidents@asoc.usda.gov or 1-866-905-8880.

"Protect It Like Your Own"

	STEP 1 Properly mark document and include name and address of recipient.		STEP 2 Use opaque inner envelope.
	STEP 3 Cover ALL envelope seams with tamper-resistant tape (e.g. duct, packing or acrylic tape).		STEP 4 Affix classification markings to inner envelope. Markings must be clear on the envelope.
	STEP 5 Address inner envelope to the recipient by name and insert into another opaque envelope. This becomes the outer wrapping.		STEP 6 Recipient's name is optional if hand carrying, but it is required when sent via U.S. Postal Service certified or any authorized delivery service (e.g., US Parcel Service, Federal Express, DHL, or private courier).



United States Department of Agriculture