USDA

FEB 22 2007

United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue SW

Washington, DC 20250

TO: Agency Administrators

FROM: David M. Combs
Chief Information Officer

SUBJECT: Physical Transport of Personally Identifiable Information

In light of recent events involving the physical transport of Personally Identifiable Information (PII), this memorandum serves as a reminder to all USDA agencies and staff offices of their responsibilities to protect PII data. PII data means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which 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 which is linked or linkable to an individual. Agencies and staff offices need to ensure that controls exist to protect the transport of PII data via electronic or physical means.

When possible, agencies and staff offices should transport PII and other sensitive information electronically using a National Institute of Standards and Technology (NIST) approved encryption method. The electronic delivery of encrypted PII reduces the risk that human error will result in the unintentional disclosure of PII or other sensitive data.

However, when physical transport of data is necessary, portable media containing PII or other sensitive data must be encrypted first, then transported by the United States Postal Service or another authorized delivery service (e.g. United Parcel Service, Federal Express, DHL, or private courier). 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 decryption key must be transmitted via a separate package or alternate channel. The package must be sent via a certified carrier with an ability to track pickup, receipt, transfer, and delivery. When necessary, portable media may be transmitted by interoffice mail provided it is double-wrapped to afford sufficient protection against inadvertent or unauthorized access.

If you have any questions or need further clarification, please call the Computer Security Operations Division, OCIO, at 816-926-7330.

Attachment
Excerpt from the Privacy Act

*Excerpts from the Privacy Act
Link: http://www.epic.org/privacy/laws/privacy_act.html

(d) Access to Records. - Each agency that maintains a system of records shall -

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of -

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

i)(1) Criminal Penalties. - 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 the disclosure of which is prohibited by this section or by rules or regulations established thereunder, 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.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.