Information Resources and Technology Management (IRTM)
Tips for Safeguarding
Personally Identifiable Information (PII) Consistent With the Privacy Act

June 2008

In December 2006, Federal Computer Week reported that the Privacy Rights Clearinghouse tallied more than 97.3 million records containing sensitive personal information that were compromised in computer-related breaches in the prior 20 month.

The FBI calls identity theft one of the fastest growing crimes in the United States and currently estimates that as many as 500,000 to 700,000 Americans become identity theft victims each year. The loss of personally identifiable information (PII) and the impact of security breaches of systems that contain PII are felt on a daily basis. Identity theft is a federal crime. It occurs when one person's identification (which can include name, social security number, or any account number) is used or transferred by another person for unlawful activities.

Attached is a short list of ***Do and Don't*** tips for safeguarding PII. We encourage <u>all</u> employees to become familiar with the list – particularly those employees who currently work with Privacy Act systems and or have systems that contain PII.

Unfortunately some identity theft incidents involve the Government and its practices related to collection, maintenance and use of PII. Although identity theft is currently a growing and media-focused issue, rules to protect the information that is the 'root' of the issue are addressed under the Privacy Act of 1974 (5 U.S.C. 552a). Those well-defined rules place responsibility on the Government for the federal collection, maintenance, retrieval and storage of such information under the Privacy Act. A Privacy Act system is a system of records (paper or electronic) in which personal information is collected, maintained and/or retrieved by an identifying symbol unique to an individual (such as name, social security number, employee number, fingerprint).

- **<u>Do:</u>**

1) Collect the minimum amount of personal information from the public and or other employees and only if it is necessary to accomplish your business objectives.

2) Keep such personal information for the minimum amount of time necessary and ensure it is timely, accurate, relevant and complete.

3) Inventory record systems, critical computing systems, and storage media to identify those containing *personal information* and be certain they have the necessary documents to authorize such collection (Privacy Impact Assessment, Privacy Act notice, narrative statement).

4) Use appropriate physical and technological security safeguards including:

a) Do not take PII out of the office without authorization and encryption.

b) Do not leave PII out unsecured on your desk.

c) Lock up and/or password protect PII when it is not in use.

d) Report any actual or suspected breach of PII immediately to the Privacy Act Officer the Incident Management Team. The FWS/National Incident Management Team points of contact are provided at: https://intranet.fws.gov/region9/irtm/bsm/sec_contacts/contacts_iitsm.php. The FWS Bureau Privacy Officer and Alternate are: Johnny Hunt, 703-358-2504 and Teri Jackson, 703-358-2257, email: **FW9Privacy@fws.gov**

5) Pay particular attention to protecting personal information on laptops and other portable computers and storage devices. (As a general rule: DO NOT store PII on such devices).

6) Have your employees, contractors, volunteers:
   a) Take the Privacy Act computer-based training;
   b) Follow bureau security policies; and,
   c) Include Privacy Act clauses/requirements in their written contracts/agreements.

7) Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information

8) Have a record of access and/or an audit trail of electronic systems with personally identifiable information in order to ensure the authenticity of the record and to record any amendments to the record.

9) Use data encryption in combination with host protection and access control wherever feasible.

10) Dispose of records and equipment containing personal information in a secure manner (and in accordance with Departmental instructions).

11) Review your security plan at least annually or whenever there is a change in business practices that may implicate or jeopardize personal information.

12) Have a breach notification policy in place. Additional sources of Privacy, PII and Security information are provided below:

http://www.myinterior.doi.net/ocio/imd/ocio_privacy_safeguard.html
http://www.myinterior.doi.net/ocio/imd/privacy/PriLeaders_trifold.pdf
http://www.fws.gov/irm/bpim/privacy.html

- **Don't:**

1) Don't collect personal information unless you can point to a Privacy Act system of records that authorizes it.

2) Don't collect social security numbers when there is an alternative identifying particular

3) Don't be afraid to ask the Bureau or Regional Privacy Act Officer's about any questions if you are uncertain.

4) Don't design an electronic system unless you have completed a Privacy Impact Assessment (PIA).

5) Don't implement an electronic system for which a PIA reveals there is personal information without first having published a Privacy Act notice.

6) Don't modify an existing Privacy Act system – unless you have checked with the Privacy Act Officer.

7) Don't access or share PII unless you are clearly authorized to do so.

8) Don’t send e-mails with PII without it being encrypted.