TELEWORK FACT SHEET

FS 12-09: Privacy Act and Protecting Information for Teleworkers

January 2012

1. Why is privacy a special concern for teleworkers?

When you take government records to a telework site, such as your home, you have in your possession official government records which require preservation and safeguarding under federal law. The safeguards that are in place in a government facility or on government computers may not be available at your home or at a telework center. The Privacy Act expressly requires that PII be secured to protect the confidential, integrity and availability of the data. So you need to understand your responsibilities under the Privacy Act and other federal statutes and regulations to protect the privacy sensitive records in your possession.

2. What do you mean by *Personally Identifiable Information*?

Personally Identifiable Information (PII) refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Not all PII is sensitive – for example, your name, official title, official address, phone number and email address are not sensitive.

Examples of PII that are sensitive include full or truncated Social Security numbers, dates of birth, addresses, phone numbers, email addresses, credit card numbers, financial information, mother's maiden name, biometric identifiers, medical information, passport number, driver's license number, and performance ratings. You should also consider context as non-sensitive PII can become sensitive when combined with other information. For example, a list of names of employees within your office as opposed to a list of names of employees with poor performance evaluations.

3. What do you mean by *Privacy Act records*?

Privacy Act records are records about individuals that are contained in a Privacy Act system of records managed by a Federal agency. You and your supervisor must coordinate with Bureau/Office Privacy Act Officers to determine whether records contained in a Privacy Act system of records may be used for telework. Examples of Privacy Act systems of records managed by the Department include:

- DOI-16, DOI Learn

- DOI-45, Personnel Security Files
- DOI-85, Payroll, Attendance, Retirement, and Leave Records

4. How do I obtain approval to work with *Privacy Act records*?

You must obtain approval from your supervisor to work with Privacy Act records from a telework location. You and your supervisor must ensure that adequate safeguards are in place to protect the records for unauthorized disclosure. Although the decision to allow the use of Privacy Act records for telework is delegated to individual supervisors, you are directly responsible for protecting the sensitive privacy data in your custody and may be held responsible for any unauthorized disclosure of that data.

Telework employees are not authorized to maintain a Privacy Act system of records at their home or alternate workplace. Failure to ensure the protection of sensitive information at the alternate workplace may result in termination of the Telework Agreement and disciplinary action.

5. How do I properly safeguard sensitive privacy data?

You must take steps to ensure that records subject to the Privacy Act and sensitive PII are not disclosed to anyone except to those who are authorized access to such information. Hard copy records and media containing privacy or other sensitive data must be physically secured at all times. You must work with your supervisor to ensure the physical, technical and administrative safeguards are in place protect the data.

- Computers, portable media, and other devices that store PII must be encrypted
- Encrypt PII during electronic transmission, transportation and storage
- Use strong passwords and do not choose options that allow your computer to remember passwords, and do not share your passwords with anyone
- Mark or label files, file cabinets, mobile storage media, etc. with the DOI Privacy Act Notice
- Physically secure PII in locked file cabinets, drawers, desks, or other secure containers
- Limit access to records or media that contain PII, and ensure data is handled, stored and safeguarded at all times to protect against loss or unauthorized disclosure
- Prevent “shoulder surfing” and lock your screen when you step away from the computer
- Do not leave PII unattended on a desk, printer, copier or fax machine
- When portable media is no longer required for storage of sensitive data, the storage device must be returned to DOI and the sensitive data degaussed or overwritten in accordance with DOI IT security policy
- Immediately report any loss or unauthorized disclosure of PII to your supervisor

6. What do I do when I leave DOI?

Upon your departure from DOI, you must return or electronically transmit all records back to your supervisor at your official duty station to be incorporated into your bureau/office's official recordkeeping system. If your official duty station is your home office or federal telework center, you must return or electronically transmit all records to your designated supervisor. Any records subject to the Privacy Act must be returned to the official location for the system of records under the control of the Department or bureau/office system manager. You must return all computer equipment and portable media to DOI to be degaussed or overwritten in accordance with DOI IT security policy.

7. Other than understanding safeguards, what else should I know?

While you have possession of government records, whether you are teleworking or on official travel, you must ensure they stay in your custody. You must safeguard all information, including sensitive data, removed from your official duty station and information created at your alternative workplace in accordance with the Federal Records Act, Privacy Act, FOIA, other Federal laws, regulations, and current DOI policies.

8. What do you mean when you say that the records must stay in my custody?

When we say records "must stay in your custody" we mean that you must secure the records under your control and cannot leave them exposed or unattended without proper safeguards. For example, you should never give government records to a non-government employee or a contractor who has no authority to handle the records. This means your friends and family members should not handle government records, so don't leave them on your home desk where your family can view or access them.

Also, when you travel with government records, be sure to secure them if they are not in your immediate possession. For example, if you are staying in a hotel room and go to dinner, be sure you secure records so that hotel personnel with access to your room cannot handle the records.

9. How do I report the loss of Privacy Act data?

Any potential loss, theft or compromise of PII or sensitive data, whether suspected or confirmed, or loss of DOI equipment, must be reported immediately to your supervisor, respective helpdesk personnel and IT Security staff. Incidents may be reported 24 hours a day to the DOI Computer Incident Response Center (DOI-CIRC) by phone at 703-648-5655 or email at DOICIRC@ios.doi.gov. DOI CIRC personnel are required to report all potential losses, theft or compromise of PII within one (1) hour to the United States Computer Emergency Readiness Team (US CERT).

10. What are the penalties for not safeguarding Privacy Act records?

If you knowingly and willfully make an unauthorized disclosure of records subject to the Privacy Act, or you willfully maintain a system of records without meeting the notice requirements, you may be subject to a misdemeanor and fined up to $5,000 (5 U.S.C. 552a; 383 DM 9). You may also be subject to disciplinary action in accordance with 370 DM 752.

11. Who can I contact for information on protecting privacy?

Your Bureau/Office Privacy Act Officer will assist you with any privacy issues while teleworking. A list of Bureau/Office Privacy Act Officers is available at http://www.doi.gov/ocio/privacy/doi_privacy_act_officers.htm.