DEPARTMENT OF ENERGY
Privacy Awareness Training

The Privacy Act

&

Safeguarding Personally Identifiable Information (PII)

PRIVACY PROGRAM

Purpose

This training is designed to address the importance of privacy, and to ensure that DOE employees are aware of the vital role they play in safeguarding privacy and protecting Personally Identifiable Information (PII).

PRIVACY PROGRAM

Privacy & PII is a Special Area of Interest at DOE

Recent breaches of PII across the government, including some at the Department of Energy, were well publicized, costly, and prompted the Administration and Congress to take action to improve the protection of PII.

Privacy Act

- The Privacy Act of 1974 (5 U.S.C. 552a) establishes controls over what personal information is collected and maintained by the Executive Branch and how the information is used.
- The Privacy Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.

Privacy Act

All DOE employees and contractors are subject to the Privacy Act and must comply with its provisions.

Non-compliance with the Privacy Act carries criminal and civil penalties.

Privacy Act

The Privacy Act requires agencies to—

- Maintain only information that is both relevant and necessary to accomplish DOE's mission.
- Publish the existence of any set of records (also known as a "System of Records") maintained on individuals that is accessed by a personal identifier, such as an individual's name or Social Security number (SSN).
- Establish "rules of conduct" for persons involved in the design, development, operation, or maintenance of any System of Records, as well as the consequences of non-compliance.

Privacy Act

Who is covered by and what records are subject to the Privacy Act?

- The Privacy Act applies to records collected and maintained on individuals who are—
  - U.S. Citizens, or
  - Lawfully admitted aliens.
- Records maintained in an agency file (either hard copy or electronic) and retrieved by a personal identifier (e.g. name, Date of Birth, SSN, fingerprint, etc.).

Privacy Act

What is a *System of Records Notice* (SORN)?

- A SORN is published in the *Federal Register*. SORNs inform the public about data that a Federal agency collects on individuals, provide the purpose and authority for doing so, and set forth the rules that DOE will follow in collecting and maintaining that personal data.
- DOE uses a SORN to notify the public of the existence of a "System of Records." A compilation of all SORNs is published by the Department on a periodic basis.

Privacy Act

What are the penalties for violating the Privacy Act?

- Both criminal and civil penalties are addressed in the Privacy Act for non-compliance.
- You may be liable if you knowingly and willfully—
  - Obtain or request records under false pretenses,
  - Disclose privacy data to any person not entitled to access, or
  - Maintain a "System of Records" without meeting *Federal Register* notice requirements.

PRIVACY PROGRAM

Privacy Act

What are the penalties for violating the Privacy Act?

- The penalty is a misdemeanor criminal charge and a fine of up to $5,000 for each offense and/or administrative sanctions.
- Courts may also award civil penalties.

Privacy Act

Accessing Records

- Requests for information protected by the Privacy Act must be made in writing and signed. Where possible, the request should also identify the applicable DOE SORN that contains the information.
- Exemptions: The Privacy Act provides exemptions under which DOE may withhold certain kinds of information.
- Contact your local DOE Privacy Act Officer for more assistance.

Privacy Act

DOE employees shall—

- Ensure personal information contained in a System of Records, to which they have access to or are using to conduct official business, is protected to ensure security and confidentiality.
- Not disclose personal information except as authorized.
- Report any unauthorized disclosures to your supervisor or local Privacy Act Officer.

Privacy Act

DOE managers shall—

- Ensure all personnel who either have access to a System of Records or who develop/supervise procedures for handling records are aware of their responsibilities for protecting personal information.
- Prepare promptly any required new, amended, or altered SORNs and submit them through the DOE Chief Privacy Officer for publication in the *Federal Register*.

Privacy Act

Helpful Tips

- Label Privacy Act protected records “OFFICIAL USE ONLY” and “PRIVACY ACT DATA”
- Report any loss or unauthorized disclosure immediately
- Do not collect personal information without proper authority

Privacy Act

Helpful Tips

- Collect only the minimum amount of PII necessary for carrying out the mission of DOE
- Do not place Privacy Act protected data on unrestricted shared drives, intranets, or the Internet
- Challenge anyone who asks to see Privacy Act data

What is PII?

DOE Order 206.1, *Department of Energy Privacy Program*, defines PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

Understanding & Safeguarding PII

Loss of PII—

- Can lead to identity theft (which is costly to the individual and the Government),
- Can result in adverse actions being taken against the employee who loses PII, and
- Can erode confidence in the Government's ability to protect personal information.

Safeguarding & Handling PII – **The Do's**

- **DO** make sure all personal data is marked "OFFICIAL USE ONLY"
- **DO** report immediately any loss (or suspected loss) or unauthorized disclosure of PII to your supervisor, program manager, Information System Security Manager, or Privacy Act Officer
- **Do** report any suspected security violation or poor security practices relating to personal data
- **DO** lock up all notes, documents, removable media, laptops and other materials containing personal data when not in use

PRIVACY PROGRAM

Safeguarding & Handling PII – **The Do's**

- **DO** log off, turn off, or lock your computer whenever you leave your desk
- **DO** protect personal data from unauthorized use
- **DO** encrypt personal data sent via email
- **DO** destroy personal data via shredder when no longer needed and retention is not required
- **DO** be conscious of your surroundings when discussing personal data—protect verbal communication with the same heightened awareness as you would paper or electronic data

Safeguarding & Handling PII – **The Don'ts**

- **DON'T** leave personal data unattended
- **DON'T** take personal data home, in either paper or electronic format, without written permission of your manager or other authorizing official, as required
- **DON'T** discuss or entrust personal data to individuals who do not have a need to know

Safeguarding & Handling PII – **The Don'ts**

- **DON'T** discuss personal data on wireless or cordless phones (unless absolutely necessary)
- **DON'T** put personal data in the body of an email; rather, password-protect it as an attachment
- **DON'T** dispose of personal data in recycling bins or regular trash unless it has first been shredded

Summary

- **Each DOE employee needs to be aware of their responsibilities to—**
  - protect personal information,
  - avoid unauthorized disclosures of personal information,
  - ensure that no records about individuals are maintained without proper public notice in the *Federal Register,* and
  - report immediately any loss or misuse of personal information.
- **Questions should be referred to your supervisor, your local Privacy Act Officer, or the Privacy Office (MA-90) at (202) 586-5955.**

Certification of Privacy Awareness Training

"This is to certify that I received Privacy Awareness Training. I understand that I am responsible for safeguarding personal identifiable information that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or unauthorized disclosure of such information."

_____ _____/____

(Print Name) (Signature) (Date)