DEPARTMENT OF ENERGY
Awareness Training

PRIVACY ACT
&
Safeguarding Personal Identifiable Information (PII)

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 ensuring that PII is protected from unauthorized disclosure.
- Part I of the training provides an overview of the Privacy Act and Part II includes guidance for safeguarding PII.

Privacy & PII is a Special Area of Interest at DOE

- Recent breaches of PII across the government were well publicized, costly, and prompted the Administration and Congress to take action to improve protection of PII data.

Part I:
Privacy Act Overview

- 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 Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.

Privacy Act

- DOE employees and Contractors is subject to the Act and must comply with all of its provisions.
- Non-compliance with the Privacy Act carries criminal and civil penalties.

Privacy Act
The Act requires agencies to:

- Maintain only information that is both relevant and necessary to accomplish DOE's mission;
- Publish the existence of a System of Records (and subsequent changes thereto), i.e., System of Records Notices;
- Establish "rules of conduct" for persons involved in the design, development, operation, or maintenance of any system of records; and the consequences of non-compliance.

Privacy Act
Who is covered by the Act?

- The Act applies only to records collected and maintained on individuals who are: (1) U.S. Citizens or (2) lawfully admitted aliens, whose records are filed in a "system of record" where those records are retrieved by a personal identifier.

Privacy Act
What Records are subject to the Act?

- Records about an individual collected and maintained in a “system of records.”
- A system of records is a group of records that: contains a personal identifier (e.g., name, DOB, SSN, fingerprint, etc.); includes at least one other item of personal data (e.g., address, performance rating, etc.); and is structured so that data about an individual is retrieved by their personal identifier(s).

Privacy Act

What is a “System of Record Notice (SORN)”?

- DOE is required by the Act to publish the existence of a “system of record” in the Federal Register; this is called a SORN.
- The SORN informs the public what data is collected, the purpose and authority for doing so and sets the rules that DOE will follow in collecting and maintaining the personal data.

Privacy Act
What are the penalties for violating the Act?

- Criminal and civil penalties are addressed in the Act for non-compliance.
- You may be liable if you knowingly and willfully (1) obtain or request records under false pretenses, (2) disclose privacy data to any person not entitled to access, or (3) maintain a "system of records" without meeting Federal Register notice requirements.
- Penalty: 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 in a "System of Records"

- Requests for information must be in writing and signed, addressed to the appropriate DOE activity maintaining the information, identify the applicable DOE SORN that contains the information (contact local DOE Privacy Act Officer for assistance).
- Exemptions: The Act provides exemptions under which DOE may withhold certain kinds of information.

Privacy Act
"Rules of Conduct"

- The Act requires DOE to establish "rules of conduct" for persons involved in the design, development, operation, and maintenance of a "system of record", and the penalties for non-compliance.
- As a DOE employee, YOU play an important role in assuring that DOE complies with the Act.

Privacy Act
Rules of Conduct (cont'd)

- DOE workforce shall:
- Ensure that personal information contained in a system of records, to which they have access to or are using incident to the conduct of 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
Rules of Conduct (cont'd)

- DOE Privacy Act System Managers shall:
- Ensure that all personnel who either have access to the system of records or who develop or supervise procedures for handling records in the system of records are aware of their responsibilities for protection personal information.
- Prepare promptly any required new, amended, or altered system notices and submit them through the DOE HQ Chief Privacy Officer for publication in the Federal Register.

Privacy Act
Rules of Conduct (cont'd)

- DOE System managers shall (cont'd):
- Not maintain official files on individuals that are retrieved by name or other personal identifier without first ensuring that a Privacy Act SORN has been published in the Federal Register.

Privacy Act
Rules of Conduct – Helpful Tips

- Label Privacy Act protected records “FOR OFFICIAL USE ONLY – PRIVACY ACT DATA”
- Report any loss or unauthorized disclosure immediately
- Do not collect personal information without proper authority
- Collect only the minimum amount of personally identifiable information necessary for carrying out the mission of DOE
- Do not place Privacy Act protected data on shared drives, intranet, or internet
- Challenge anyone who asks to see Privacy Act data

PART II
Understanding & Safeguarding PII

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

Current Definition of PII

- DOE Notice 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information,* currently defines PII as: any information 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, etc., and including any other personal information that is linked or linkable to a specific individual.

Your Responsibilities

- Upon learning of a suspected or confirmed breach involving PII in printed or electronic form, report the breach to your management. In turn, your management will take necessary actions required by DOE N 206.5.
- Review the “helpful tips” on slide 16.
- Review the attached “do’s & don’ts.”

Safeguarding & Handling PII Quick Reference Guide –DO

- **DO** make sure all personal data is marked “FOR OFFICIAL USE ONLY” or “PRIVACY DATA”
- **DO** protect personal data from unauthorized use
- **DO** report any loss or unauthorized disclosure of personal data 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 medial, laptops, and other materials containing personal data when not in use
- **DO** log off, turn off, or lock your computer whenever you leave your desk
- **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
Quick Reference Guide – Don't

- **DON'T** leave personnel data unattended
- **DON'T** take personnel data home, in either paper or electronic format, without written permission of your manager or other official, as required
- **DON'T** discuss or entrust personal data to individuals who do not have a need to know
- **DON'T** discuss personal data on wireless or cordless phones (unless absolutely necessary)
- **DON'T** put personal data in the body of an email. It must be password-protected as an attachment
- **DON'T** dispose of personnel related data in recycling bins or regular trash unless it has first been shredded

Summary

- Each employee of DOE needs to be aware of their responsibilities under the Privacy Act to protect personal information; avoid unauthorized disclosures; ensure that no system of records retrieved by personal identifier is maintained without proper public notice in the Federal Register; and report any loss or misuse of personal information.
- Thank you for completing the training!
- Print & Sign the following certificate and provide a copy to your supervisor.

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)