Personally Identifiable Information and Privacy Act Responsibilities

Awareness Course

Introduction

- This training is designed to ensure that NRC staff understand their responsibilities under the Personally Identifiable Information (PII) policy and Privacy Act of 1974.
- In accordance with the Office of Management and Budget (OMB) memorandum (M-07-16), "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007, Federal agencies are required to ensure that all individuals are:
  - Aware of the responsibilities relative to protecting PII
  - Aware of the consequences and accountability for violation of these responsibilities
  - Acknowledge this understanding at least annually

Objectives

By the conclusion of this training, you will be able to:

- Identify the privacy responsibilities of Federal employees.
- Identify the appropriate use of information relative to the protection of information.
- Identify examples of information that might be considered PII.

What is PII?

PII is information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual.

PII is a person's name, in combination with any of the following information:

- Mother's maiden name
- Driver's license number
- Bank account information
- Credit card information
- Relatives' names
- Postal address
- E-mail address
- Home or cellular telephone number
- Personal characteristics
- Social Security Number (SSN)
- Date or place of birth
- Other information that would make the individual's personal identity easily traceable

What is not PII?

Since personal identity is distinct from an individual's professional identity, the NRC does *not* treat the following information as PII:

- An individual's name
- An individual's title
- Work telephone number
- Official work location/address
- Work e-mail address

Is all PII Protected?

No, the NRC does not require the protection of the following PII:

- Home addresses, home phone numbers or home e-mail addresses contained in adjudicatory filings, documents associated with agency rulemakings, and correspondence received from the public on regulatory matters.
- Emergency contact lists containing PII, such as names, home and cellular phone numbers, and home e-mail addresses may be carried in paper form or stored in personal electronic devices outside of NRC-controlled space.

Why Do You Need to Know about PII?

- It is information about individuals that the Federal Government collects, maintains, distributes, and destroys. It includes information about you.
- You must take precautions when handling PII in the performance of your job.
- The loss of, or unauthorized access to, PII can result in:
  - Substantial harm, embarrassment, and inconvenience to individuals, as well as our agency
  - Identity theft

Do Not Collect or Maintain PII

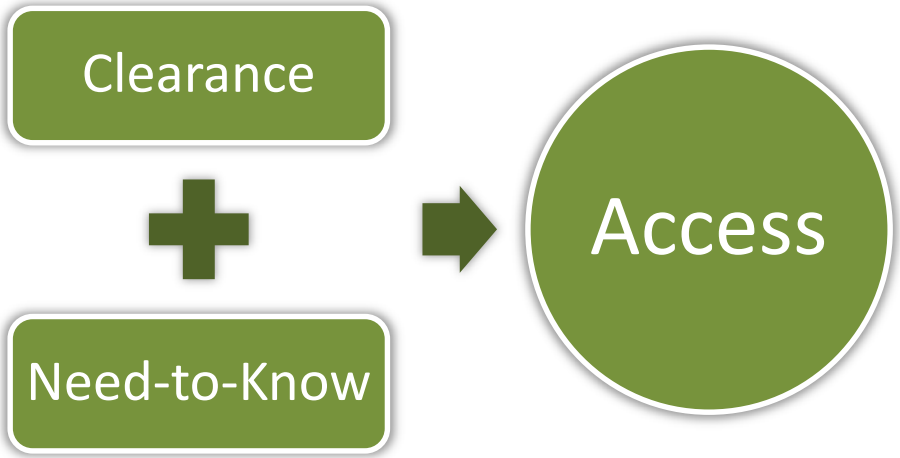
Do not collect or maintain PII unless you are authorized to do so as part of your official duties. Even then, you should only collect and retain PII that is relevant and necessary for NRC functions or responsibilities.

Use Authorized System of Record

Ensure that PII retrieved by an individual's name or other personal identifier is maintained in an authorized Privacy Act (PA) system of records for which a system notice has been published in the *Federal Register*.

Verify Need-to-Know

Only disseminate PII to those NRC employees who have a need-to-know the information to perform their official duties, not want-to-know.



Do Not Disclose PII

Do not disclose PII to anyone outside of the NRC unless the disclosure is authorized for the purpose of conducting official business.

This does not prohibit you from disclosing your own PII.

All NRC Forms Must be Reviewed for Privacy

- All NRC forms must be reviewed to see if they contain PII by the Privacy Team in the Office of Information Services.
- The Privacy Team determines if the form will need to have a Privacy Act Statement.
- Forms may not be used to collect information until the Privacy Team has reviewed them.
- Submit NRC forms for review to: Forms.Resource@nrc.gov

Protect the Information

Maintain PII in a manner that will prevent inadvertent or unauthorized disclosures.

- Do not leave PII in open view of others, either on your desk or computer screen.
- Use an opaque envelope when transmitting PII through the mail.
- Secure paper records in a locked file drawer and electronic records in a password protected or restricted access file.
- Do not place or store PII on a shared network drive unless access controls are applied.

Do Not Transmit PII

Do not e-mail or otherwise transmit PII outside of the NRC's infrastructure except where essential to conduct agency business. E-mailing PII to those with a need-to-know within the NRC local area network/wide area network is acceptable, including to and from BlackBerry hand-held devices interacting within the NRC's e-mail system.

Do not remove paper documents that contain PII of individuals, other than yourself, from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted. This does not apply to emergency contact information.

Do not remove electronic PII from NRC-controlled space on mobile information technology (IT) devices, such as CDs, DVDs, or thumb drives unless all PII is encrypted.

Rules of Behavior for Authorized Computer Use

When using or accessing electronic PII, follow the NRC Agencywide Rules of Behavior for Authorized Computer Use.

Properly Destroy and Dispose of PII

- Properly destroy and dispose of PII that is no longer required.
- Do not place in regular trash or recycle bins.
- Before destruction, refer to the NRC records disposition schedules for applicable retention schedules.

Social Security Numbers

OMB M-07-16 and the Office of Personnel Management's memorandum dated June 18, 2007, require agencies to reduce the unnecessary use of the SSN.

- Eliminate the unnecessary collection or retention of SSNs.
- Eliminate the unnecessary use of SSNs as an identifier.
- Eliminate the unnecessary printing and displaying of SSNs on forms, reports, and computer display screens.
- Restrict access to SSNs only to those individuals whose official duty requires such access.

Is PII Protected under the Privacy Act?

Only PII that is included in a PA system of records will be protected by the provisions of the PA; therefore, while some PII is PA information, much of it is not.

PII that is contained in documents, files, or databases not part of a PA system of records will not receive the legal protection of the PA, but you must still treat it in accordance with National Archives and Records Administration direction and applicable NRC policy for handling PII.

Violations

In accordance with the existing authority, the NRC may impose progressive disciplinary measures on employees for infractions of the agency's PII policy.

Violations involving security controls, unauthorized disclosure, unauthorized access, reporting requirements, and supervision may constitute a basis for a disciplinary action, including reprimand, suspension, removal, or other actions consistent with applicable law and policy.

In addition, appropriate legal action may be pursued for breaches of NRC PII caused by non-NRC employees, such as NRC contractors.

Types of Violations

Security Controls Violation

Failure of the responsible employee to implement and maintain applicable PII security controls of which the employee is aware, regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

Unauthorized Disclosure Violation

Deliberate, unauthorized disclosure of PII to others. Infractions involving PA violations (willful disclosure of PA information to unauthorized recipient(s)) may result in criminal prosecution under the PA. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

Unauthorized Access Violation

Deliberate, unauthorized access to or solicitation of PII. Infractions involving PA violations (requests for access to PA information under false pretenses) may result in criminal prosecution under the PA. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

Reporting Requirements Violation

Failure to report any known or suspected loss of control or unauthorized disclosure of PII.

Supervision and Training Violation

Failure, as a manager, to adequately instruct, train, or supervise employees in their responsibilities.

Report Suspected or Confirmed Inadvertent Breaches

Use step 1 or 2 below as applicable:

1. Any release of PII where IT equipment/system is involved must be reported immediately to the Computer Security Office's (CSO) Computer Security Incident Response Team (CSIRT) at CS_IRT@nrc.gov or 301-415-6666.
2. Situations involving the improper handling or storage (no IT equipment/system involved) of PII must be reported immediately to the Office of Administration (ADM), Division of Facilities and Security (DFS) or the Duty Officer at ADM/DFS: DFS_RPT@nrc.gov or 301-415-6184. After hours, contact the Duty Officer through the Central Alarm Station: 301-415-2056 or 301-415-2200.

Report Suspected or Confirmed Deliberate Breaches

In addition to the steps for an inadvertent release, any potentially deliberate breach of PII requires immediate notification of the Office of the Inspector General (OIG) at 301-415-5930 or 301-415-5925, or the OIG Hotline at 800-233-3497.

Any other notifications or actions must be approved by the OIG under these circumstances as any action may impede their investigation.

Knowledge Check #1

Directions: Read the question below and select the best answer.

Question

Your NRC team leader asked you to compile an emergency contact list with the name, home or cellular telephone number, and e-mail address of the members of your team. How do you respond?

Choices

- **Create the list, save it in the agency network shared drive, and restrict access to only the members of your team.**
- Create the list and save it in your office's G drive.
- Create the list and post it to the bulletin board in the coffee break area.
- Tell your team leader that the list would contain PII; therefore it cannot be created.

Knowledge Check #2

Directions: Read the question below and select the best answer.

Question

You are looking for a trip report in your office's network shared drive. You come across a file entitled “Travel Information.” When you open the file looking for the trip report, you see a document containing names and credit card numbers of some of your coworkers. What should you do?

Choices

- Immediately report this to your supervisor as a PII spill, in accordance with inadvertent release reporting policies.
- Notify your IT coordinator to remove the document or place access restrictions on it.
- Report the compromise to CSIRT.
- **All of the above.**

Summary

In this course, you have learned how to:

- Identify examples of information that might be considered PII.
- Identify the responsibilities of Federal employees to protect PII.
- Identify the unauthorized release of PII and reporting requirements.