Privacy 101

Awareness and Best Practices

GPO

Protection of Personally Identifiable Information (PII)

- **National Institute Of Standards & Technology**

- **What is Privacy**

  It is more than "information security" "Privacy" requires us to consider additional rights and interests of individuals in their data, such as **notice, choice, due process, and remedies**.

  It is more than "information security" **Information security is primarily about protecting data in order to preserve its "confidentiality, integrity, and availability"** (National Institute Of Standards & Technology, Commerce Dept. — NIST)

  It is more than "information security" Because personal data can be used to determine individuals' rights, benefits, privileges, freedoms, reputation **"Privacy" recognizes that individuals must have a role in the collection, maintenance, use, and disposition of their personal data**.

Federal Data Privacy Framework

- **Privacy Act of 1974, 5 U.S.C. 552a**
  - Implemented Fair Information Practice Principles (FIPPS)
  - Responded to public concerns about covert…
  - …Government information collection activities

- **E-Government Act of 2002 (EGOV)**
  - Move Federal services and programs online
  - Encourage citizen access and participation
  - Increase transparency

- **Other Federal laws, policy, and guidance**
  - Linking Policies—OMB 05-04 (2004)
  - Protection of Sensitive Information—OMB 06-16 (2006)
  - Data Breaches—OMB 07-16 (2007)
  - Tracking/Customization Technologies— OMB 10-22 (2010)
  - Third-Party Sites--OMB 10-23 (2010)

Federal Data Privacy Framework

- **Other Federal laws, policy, and guidance**
  - Paperwork Reduction Act
  - Federal Records Act
  - Section 508 of Rehabilitation Act
- **Other Federal laws, policy, and guidance**
  - Federal Acquisitions Regulation (FAR)
  - Children's Online Privacy Protection Act (COPPA)
  - Intelligence Reform and Terrorism Prevention Act (IRTPA)
  - FRCP 5.2 (requires redaction of PII characters)
  - E-Discovery
- **Other Federal laws, policy, and guidance**
  - Health Insurance Portability & Accountability Act (HIPAA)
  - Protection of Human Subjects in Research (**Common Rule, 45 CFR Part 46**)
  - Fair Credit Reporting Act (FCRA)
  - Federal tax records laws
  - Federal Educational Rights and Privacy Act (FERPA)

GPO

Protection of Personally Identifiable Information (PII)

- **GPO Directive** 825.41

- **Purpose**

  To establish a framework for the protection of personally identifiable information (PII) at the U.S. Government Printing Office. The loss, compromise, or disclosure of PII may lead to identity theft or other fraudulent use that could result in substantial harm, embarrassment, inconvenience, or unfairness to individuals. Appropriate measures are therefore necessary to protect PII from unauthorized use, access, disclosure, or sharing and to protect related information systems from unauthorized access, modification, disruption, or destruction.

Handling Rules for PII

Paper Form

- **Storing** PII: Lock cabinets when not in use.
- **Transporting** PII: Physically between approved locations and with prior authorizations.
- **Destroying** PII: Cross cut shredding.

Electronic Form

- **Transmitting** PII: Between facilities or through e-mail
- Encrypt at rest
- Encrypt when transmitted
- Authorized users only

In accordance with **GPO Directive** 825.41.

Handling Rules for PII

Special handling required to protect privacy data or sensitive data includes:

- **Labeling**: Personally Identifiable Information (PII) as "For Official Use Only" (FOUO)
- **Accessing:** Only what is necessary to complete a work-related duty or job
- **Disclosing**: Verbal, paper, and electronic PII only within and between authorized entities to conduct official business

In accordance with **GPO Directive** 825.41.

What are PII Data Breaches?

Privacy Data Breaches are Inappropriate Disclosures of PII that may:

- Be lost, stolen, or compromised PII
- Be intentional or accidental
- Affect high-risk or low-risk PII
- Be found immediately or after a delay

Also referred to as a PII Incident

PII Incident Reporting

For the general public reporting PII incidents, use the GPO Customer help process.

- To report a privacy incident, access the GPO customer help "Ask A Question" at the GPO's public website.

  (**http://gpo.custhelp.com/cgi-bin/gpo.cfg/php/enduser/ask.php**)

- Complete the report and keep your Question Reference number once received from your email provider.

What's a PII Incident?

When personally identifiable information is discovered in publications and online content distributed or disseminated through the Federal Depository Library Program (FDLP).

PII Incident Reporting

Privacy (PII) Incident Report: Provide Details

- When reporting a Privacy (PII) incident, provide as much detailed information as possible about what occurred, when did the incident occur and what information was compromised.
- Any paper documentation, webpage URL or system process information from the breached should be reported to GPO.
- GPO will take appropriate action to mitigate the effects of the incident and report its findings as determined by the GPO Privacy Office.

3 Basic Privacy Best Practices

- Understanding the importance of PII protection.

  If you collect it, you must protect it!

- Identifying best practices for protecting & retaining PII.

  *Think **PRIVACY** when handling **PII**!*

- ***Don't keep it*** longer than needed!

  Can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identify theft or other fraudulent use of information.

Point of Contact

GPO Privacy Program

Antonio. F. David Workman, CIPP/G, CIPP/IT
Privacy Program Manager
Information Security Division
Office of the Chief Information Officer
U. S. Government Printing Office
732 North Capitol Street, N.W.
Washington, DC 20401
Privacy@gpo.gov

Thank You