Enterprise-Wide Safeguarding Personally Identifiable Information (PII) Fact Sheet

Safeguarding Personally Identifiable Information

The United States Department of Agriculture (USDA) has made a risk management decision to exclude Information Security Awareness (ISA) training for non-organizational users. USDA has determined that the cost to train non-organizational users that do not have access to USDA systems, network or sensitive data (e.g., state employees, county employees, university employees, janitorial employees, maintenance employees) outweighs the risk they pose.

This document exempts approved non-organizational users from the requirement to complete Personally Identifiable Information (PII) training. However; USDA employees, contractors, and all others working with and/or on its behalf has the legal responsibility to properly collect, access, use, safeguard, share, and dispose of PII to protect the privacy of individuals. You are the first line of defense in protecting PII and helping to prevent possible identity theft. This fact sheet provides guidance to help you safeguard PII in paper and/or electronic form during your everyday work activities.

What is PII?

PII is ANY information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as information found on a business card or official email signature block. This type of information does not require special handling. There is also PII, which if lost, compromised, or inappropriately disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. It has stricter handling requirements. Examples include: Social Security numbers (SSNs), financial account numbers, date of birth, and biometric identifiers (e.g., fingerprints and facial images). Other data elements such as citizenship or immigration status, account passwords, and medical information, in conjunction with the identity of an individual, are also considered PII. The context of the PII should be considered to determine potential risk impacts, such as a list of employees with poor performance ratings as opposed to a list of employees who completed privacy training. Note that even when an individual's name is not present it may still be PII if it can be used to identify or be linked to an individual, and PII can also be created when information about an individual is made available or combined with other information.

Legal, Federal and USDA Requirements for Protecting PII

- The mandates for you and your organization to protect PII in both hard copy and electronic format come from legal, Federal, USDA and NIST 800-122 guidance. Congress passed the Privacy Act of 1974, signed into law in 1975, to protect individuals' sensitive information. This is the primary legislation that protects PII today.
- Congress also enacted the e-Government Act of 2002, as amended. This law provides requirements for protecting Federal information, including privacy information.

- The Office of Management and Budget, or OMB, is a part of the Executive Office of the President of the United States. In this role, OMB provides guidance to the agencies of the Executive Branch of the Federal Government on how to implement these laws on protecting privacy information.
- Key OMB guidance regarding Federal agency responsibilities for maintaining records - about individuals and protecting PII includes Circular A-130 and Memorandum M-17-12.

USDA Directives Supporting the Privacy Act

The USDA implements the Privacy Act through guidance in the "USDA Privacy Program," as contained in the following Departmental Manuals (or DMs):

- DM3515-000 Privacy Requirements (Feb. 17, 2005)
- DM3515-002 Privacy Impact Assessment (Feb. 17, 2005)
- DM3550-002 Sensitive but Unclassified Information Protection (Feb. 17, 2005)
- DM3550-003 Portable Electronic Devices and Wireless Technology (Feb. 8, 2006)
- DM3545-001 Computer Security and Training Chapter 9, Part 1 (Feb. 17, 2005)

The following Office of the Chief Information Officer Memoranda:

- Minimum Safeguards for Protecting Personally Identifiable Information (Nov. 20, 2018)
- Reporting Personally Identifiable Information to United States Computer Emergency Response Team (US-CERT) (Feb. 24, 2010)
- Logging and Handling of Data Extracts of Sensitive Information and Personally Identifiable Information (Apr. 12, 2010)
- Sanitizing Multifunctional Devices to Safeguard Sensitive But Unclassified and/or Personally Identifiable Information (Aug. 2, 2011)

The USDA Privacy Program affirms that the privacy of an individual is a personal and fundamental right that should be respected and protected. Further, USDA personnel, including contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual. USDA's privacy policy is located at https://www.usda.gov/privacy.

Noncompliance Violations and Penalties

Violating the Privacy Act has serious implications for you and your agency.

You can be charged with a criminal penalty for keeping what is called a System of Record without publishing it in the Federal Register. A System of Record consists of records that are retrieved by the name of an individual or some other personal identifier. A database of personnel files is an example of a System of Record.

Additionally, a person can be prosecuted for asking for, or taking, information under false pretenses. Knowingly and willingly giving someone else's PII to anyone who is not entitled to it

is also a violation. Failure to comply with the Privacy Act can result in a misdemeanor criminal charge as well as a fine of up to $5,000 for each offense.

Organizations are also held accountable for their employees' failures to protect PII. For example, if an individual is unable to gain access to their record or to update the information, the agency may not be complying with the law. If the agency's employees fail to maintain accurate, relevant, timely and complete data, the agency is violating the law.

It also violates the Privacy Act when a person is harmed by a failure to safeguard sensitive data. Civil penalties apply to Federal agencies, not the employees. If an agency is found to be noncompliant with the Privacy Act or an agency's rules, the organization has to pay actual damages and reasonable attorney fees.

This does not mean that Federal employees who commit violations will not face penalties. It is possible for the Federal Government to prosecute an employee on criminal charges. In addition, USDA disciplinary penalties include a letter of reprimand to removal for "unauthorized disclosure or use of (or failure to safeguard) information protected by the Privacy Act or other official, sensitive, or confidential information."

Breach Notification

A breach includes the loss of control, compromise, unauthorized disclosure, acquisition, or access by someone who is not allowed access to that PII. OMB defines a breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses PII, or an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Reporting a PII Incident

You should immediately report suspected or confirmed PII incidents to the PII hot line at 1-877-PII-2-YOU, or 1-877-744-2968. The hotline is operational twenty-four hours a day, seven days a week. You can also e-mail cyber.incidents@ocio.usda.gov or contact the ASOC Hotline at (866) 905-6890.

I acknowledge receipt of the Enterprise-Wide Safeguarding Personally Identifiable Information (PII) Fact Sheet and I understand my responsibilities and will comply with my responsibilities to protect PII.

_____ _____

Signature Date