INFORMATION DIRECTIVE
PROCEDURE

Protecting Sensitive Personally Identifiable Information (SPII)		
Directive No.: 2151-P-10.0	CIO Approval: 12/19/2016	Transmittal No.: 17-001

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Protecting Sensitive Personally Identifiable Information

1. PURPOSE

The purpose of the procedure is to ensure the adequate protection of Sensitive Personally Identifiable Information (SPII): a) from inadvertent disclosure when collecting, accessing and disclosing it to authorized personnel; b) when being accessed from outside the Agency; c) when removed physically from an EPA location for authorized and approved purposes; and d) when maintained within the Agency.

2. SCOPE

The procedure applies to any SPII (e.g., Social Security Number (SSN), biometric, passport, medical or financial information associated with an individual) in an EPA facility or information system used by EPA, whether onsite, offsite or accessed remotely.

3. AUDIENCE

The procedure applies to all EPA employees, contractors, grantees and other persons authorized or entrusted with the stewardship of SPII.

4. BACKGROUND

Without proper security and access controls, SPII collected by agencies is vulnerable to unauthorized access and use that could lead to identity theft. Security and controls, as outlined in CIO-2150-P-01.2 Information Security- Access Control Procedure, are required to protect this information due to the harm it could cause if breached.

The Office of Management and Budget (OMB) states agency practices should guard against unauthorized disclosure or misuse of SPII (in paper and electronic formats). OMB Memorandum M-06-16 "*Protection of Sensitive Agency Information*" directed each federal department and agency to review and determine their baseline activities for the protection of SPII and ensure appropriate safeguards are in place.

SPII is a subset of Personally Identifiable Information (PII), which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual. EPA has three categories of PII classified as sensitive: 1) SSN or comparable identification numbers, 2) biometric data, and 3) financial information or medical information associated with an individual. SPII requires additional levels of security controls.

OMB M-06-16 provides a Security Checklist to ensure the protection of information when information is removed or accessed from outside the agency's physical location. Agencies were directed to: confirm identification of SPII protection needs; verify adequacy of organizational policy; implement protection for SPII being transported and/or stored offsite; and implement protections for remote access to SPII.

The Federal Information Security Modernization Act (FISMA) of 2014 requires an annual report on how agencies plan to reduce and/or eliminate the use of SSNs. Agencies must review their use of SSNs in agency systems and programs to identify instances in which the collection or use of the SSN is superfluous. Agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of SSNs. EPA's plan to eliminate usage of unnecessary SSNs is posted at: http://www2.epa.gov/privacy/omb-directives-about-privacy-act-and-federal-agency-privacy-policies.

5. AUTHORITY

The information directive is issued by the EPA Chief Information Officer, Pursuant to Delegation 1-19, dated 07/07/2005.

Additional legal foundations for the procedure include:

- Privacy Act of 1974, USC 552a
- E-Government Act of 2002, 44 USC 3501 et seq.
- Federal Information Security Modernization Act of 2014 (FISMA)

6. PROCEDURE

EPA's Chief Information Officer (CIO) issued policy and procedures to address the critical issue of protecting SPII (CIO Policy Transmittal 15-013) on September 14, 2015.

While ideally employees should only work with SPII within the confines of EPA's offices, labs and only on the Agency's computer network, in those instances where it is determined the remote access of SPII, or the removal and/or local storage of SPII is necessary, the procedures contained herein must be applied. When teleworking, there must be a legitimate business need and written approval from the EPA organization's Senior Information Official (SIO) only when the individual will be accessing Agency SPII.

General Guidance

The following requirements apply to all EPA employees, contractors, grantees and other persons authorized or entrusted with the stewardship of SPII:

- EPA will not collect or use a SSN as an access element or personal identifier in connection with any information system or database, unless the collection and/or use is authorized and provided for by law and an alternative access element or personal identifier is not feasible.

- The Agency Privacy Officer must approve all forms collecting PII prior to issuance of an EPA form number;
  - All Employees who telework must:
    - Certify in writing they have completed remote access training available at (http://intranet.epa.gov/epahriis/telework/training.html#employee);

- All employees must:
  - Obtain approval from the SIO if remote access is required and/or when transporting/transmitting SPII offsite. Employees must obtain written permission from the SIO of the organization using the "Request for Remote Access and Use of Sensitive PII" form;
  - Ensure all remote access and mobile devices have an automatic time out function requiring re-authentication after 15 minutes of inactivity;
  - Document all approved downloads and/or local storage of SPII;
  - Encrypt documents containing SPII properly (unless provided as an Enterprise solution) and document the encryption;
  - Ensure all such SPII has been erased, returned, or destroyed within 90 days, or request approval from the SIO for continued use;
  - Never send unencrypted email containing SPII;
  - Eliminate all unnecessary collections of SSNs;
  - Identify an alternative identifier to the SSN when possible;
  - Truncate or mask SSNs when displaying and printing the SSN if the SSN must be used;
  - Allow remote access only with multifactor authentication, where one factor is provided by a device separate from the computer gaining access and access is provided over an encrypted connection (e.g., VPN, SSL/TLS, etc.);
  - Use tools and procedures appropriate for individual file deletion according to EPA Procedures for Disk Sanitization for digital media; and
  - Shred paper media using a cross-cut or confetti shredder that results in remnants no larger than 5/32" x 2" or smaller as dictated by the organization, system policy or rules.
  - SPII should not be stored in the Cloud infrastructure without prior approval from the Agency Privacy Officer.
    - Agency email, which is stored in the cloud through Microsoft Office 365, is acceptable as Microsoft Office 365 has a Federal Risk and Authorization Management Program (FedRAMP)[1] Authority-to-Operate (ATO).

A. Transport of SPII

a. Hard Copy

[1] *FedRAMP is a U.S. government-wide program whose goal is to accelerate adoption of secure cloud solutions and provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

When SPII needs to be transported from the confines of EPA's offices and labs, where it is determined the remote access of SPII or the removal and/or local storage of SPII is necessary, the EPA employees, contractors, grantees and other persons authorized or entrusted with the stewardship of SPII should follow the following guidelines:

- Maintain at a designated EPA location an inventory of the information to be removed that allows for notification of affected individuals should a compromise or loss occur;
- Comply with the Agency's flexiplace policies as appropriate and submit requests to remove SPII for work to a flexiplace site using the "Request for Remote Access and Use of Sensitive PII" form; and
- Protect non-digital (e.g., paper files) SPII with the following minimum protections: Place in a closed container (e.g., sealed envelope, locked brief case, etc.) with a clearly visible and distinct EPA return address, during transport to and from the off-site location.

When a hard copy of SPII needs to be transferred between offices, it must be packaged in double envelopes and appropriately marked. The outer envelope must be marked "To Be Opened by Addressee Only" and the inner envelope must be marked "Contains SPII." When possible, these packages should be hand-delivered to the addressee. If hand-delivery is not possible, the information must be transported using a courier service that allows the package to be tracked with proof-of-delivery (e.g., certified mail, Federal Express, UPS, etc.).

b. Soft Copy

Transport of SPII data using CDs, DVDs or USB drives is allowed if the data are encrypted according to Federal Information Processing Standard (FIPS) 140-2. The approved EPA software for encrypting SPII data is the Agency standard software.

Note the following methods for transporting SPII, which <u>are not authorized</u> for use at EPA:

- Use of unencrypted mobile devices as a computer storage device to transport SPII is prohibited.
- Use of unencrypted mobile device storage media (i.e., using a mobile device as a computer storage device) is prohibited. (Note: This does not preclude the use of the standard Agency e-mail system as defined above where the message merely appears in an e-mail application as a normal message.)
- Use of other storage media that are not or cannot be encrypted according to FIPS 140-2 is prohibited.

B. Transmission of SPII

Transmission of SPII via an application or machine-to-machine transfer is allowed subject to the following requirements:

Per CIO 2150-3 EPA Information Security Policy, all systems/devices/applications must comply with federal and agency security standards and requirements, respond to agency security vulnerability alerts, and adhere to security best practices, including the continuous monitoring of security controls and compliance documentation:

- Systems/devices/applications hosted at the Office of Environmental Information's (OEI) National Computer Center (NCC) must have gone through the full Application Deployment Checklist process. NCC will provide advice and recommendations on software/hardware packages necessary to maintain the proper encryption and authentication when transferring SPII data;
- For connection to systems outside of the EPA intranet, an approved Interagency Agreement (IA) or Memorandum of Understanding/Agreement MOU/A signed by a SIO is required with the Interconnection Security Agreements (ISA);
    - EPA's Agency Privacy Officer will review all agreements covering sharing PII prior to finalizing the agreement;
- Before authorizing transfer of SPII via an application or machine-to-machine transfer, Information Security Officers must check with their system owners to ensure that all the necessary documentation and technical controls are in place and operational;

While the Agency does not recommend faxing as a method of transmitting SPII, when this method must be used, the recipient must be notified and available to receive the transmission when it arrives and the fax number must be confirmed prior to transmission. As with procedures for mailing outlined above, the fax transmission must contain a cover sheet marked "To Be Delivered to Addressee Only," "Contains Sensitive PII."

When sending SPII via email, the following requirements apply:

- No SPII data may be included in the subject line, body of an email, or as an attachment unless it is encrypted using FIPS 140-2 compliant algorithms when using the native function in Outlook Office 365;
- When sending encrypted SPII, the password to decrypt data must not be sent via email. The password must be sent via another secure method (preferably via direct voice-to-voice communications);
    - To prevent the loss of SPII via email in the event the user forgets the password to the encrypted files, the password cannot be recovered, or the encrypted files become unusable or unavailable by any other means, the sender shall place an unencrypted copy of the information contained in the sent email and the attachment somewhere on the EPA computer network or in their respective Microsoft OneDrive, which is equivalent to the F: drive and facilitates file/folder sharing.

C. Procedure for Local Storage of SPII in an Off-Site Location

- Employees are prohibited from downloading and/or locally storing SPII (e.g., storing SPII on a privately owned hard drive) unless specifically authorized in writing by the SIO;
- SPII files are to be saved only in an encrypted form;
- Non-digital (paper based) SPII must be locked and maintained in an access controlled off-site work location and must be protected from viewing while not being accessed.

D. Consequences for Violation of Procedures or Compromise (Breach) of SPII

- When penalties are contemplated through due process of law and/or the appropriate administrative processes, it must be determined if the violation, compromise or release of SPII was negligent. A determination must be made on the impact of the event(s) to the Agency, information systems, and/or affected individuals. In cases of suspected or confirmed breaches, the Agency's breach procedure should be implemented. Reporting incidents promptly is an exercise in due diligence and is a factor that will be considered in favor of the reporting individual. Report of a potential policy or procedure violation, or the potential or actual loss or compromise of SPII could result in the temporary suspension or termination of any remote access to SPII granted to the individual pending the outcome of an inquiry.
- Refer to the *Agency Conduct and Discipline Manual* for specific guidance on administrative penalties, including the Douglas Factors. Administrative penalties may range from oral admonishment to removal.
- Civil penalties and or criminal remedies and/or loss of privileges may be imposed depending on the nature and severity of the infraction or of the loss or compromise of SPII.

7. ROLES AND RESPONSIBILITIES

Agency Privacy Officer

- Conducts periodic reviews of programs and systems of SPII holdings and the administrative controls and safeguards around the information;
- Reports annually to the Senior Agency Official for Privacy (SAOP) under FISMA;
- Conducts annual data calls for elimination of SSN;
- Conducts annual data calls for the reduction of PII; and
- Conducts data calls two times per year for systems inventory updates.

Chief Information Officer (CIO)/Senior Agency Official for Privacy (SAOP)

Note: Some responsibilities reside in specific organizational offices of the CIO

- Develops policies and procedures to augment agency policies and procedures as necessary;
- Develops policies, procedures, recommendations and solutions for protecting SPII;

- Approves encryption technology and provides for an enterprise solution to encrypt SPII information; and
- Approves the Privacy Policy and Privacy Procedures.

Employees

- Implement the proper protection requirements for SPII;
- Complete all required training;
- Ensure all such SPII has been erased, returned, or destroyed within 90 days, or requests approval from the SIO for continued use;
- Complete and submits a request for remote access to SPII to the SIO.

Information Management Officer (IMO)

- Ensures that information and information technology (IT) planned, utilized and managed by OEI supports its business needs and mission and helps to achieve EPA's strategic goals; and
- Ensures compliance with policies and procedures.

Information Security Officer (ISO)

- Maintains a list of system/programs that have SSNs;
- Develops a plan to reduce all unnecessary collections of SSNs;
- Monitors systems/programs to ensure SPII elements are up-to-date and relevant; and
- Ensures all necessary documentation and technical controls are in place and operational.

Liaison Privacy Official

- Administers the day-to-day activities and responsibilities of privacy in their specific program or EPA region;
- Assists SOs with preparing privacy documentation (Privacy Threshold Analysis, Primacy Impact Assessments, System of Records Notices) for new and/or revised systems;
- Assists SOs with terminating systems when no longer maintained in accordance with proper destruction/transfer procedures;
- Assists SOs with breach responses;
- Works with Records Liaison Officers to ensure the proper disposal of PII in accordance with Agency records schedules and disposal procedures;
- Requests additional information for systems requiring SSN as identifier; and
- Submits updates to Agency inventory of systems that collect PII and SPII two times per year.

Senior Information Official (SIO)

- Reviews and approves the removal of SPII to an off-site (non-EPA) location and/or the access to SPII from a remote (non-EPA) location via the "Request for Remote Access

and Use of Sensitive PII" Form, as needed, in accordance with organizational requirements;
- Maintains a copy of the original request and remote access form;
- Provides a copy of the completed approval form to the requester's supervisor; and
- Ensures completion of required training by users and compliance with requirements.

System Owner (SO)

- Completes training specific to their systems;
- Performs periodic reviews of existing databases to determine if SPII data elements are still required;
- Ensures Privacy Impact Assessments are prepared for any system that collects SPII.
- Ensures copies and files no longer needed after 90 days are properly destroyed;
- Ensures compliance with policies and procedures;
- Prepares privacy documentation for new and/or revised systems; and
- Terminates systems in accordance with proper destruction/transfer procedures when they are no longer needed.

8. RELATED INFORMATION

- EPA's Privacy Policy
- EPA Information Security Policy
- M-01-05, Guidance of Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
- M-06-15, Safeguarding Personally Identifiable Information
- M-06-16, Protection of Sensitive Agency Information
- M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- M-11-02, Sharing Data While Protecting Privacy
- M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines
- M-12-11, Reducing Improper Payments through the "Do Not Pay List"
- M-12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- M-13-20, Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative
- M-14-03, Enhancing the Security of Federal Information and Information Systems
- M-14-04, Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

- M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services
- M-15-14, Management and Oversight of Federal Information Technology

9. DEFINITIONS

- **Access.** The ability or opportunity to gain knowledge of PII or SPII.
- **Cloud Computing.** Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- **Harm.** Loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.
- **Maintain**. Develop, update and correct as necessary.
- **Personally Identifiable Information (PII)**. Any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual (e.g., social security number, name, date of birth.)
- **Privacy Act Information**. Data about an individual that is retrieved by name or other personal identifier assigned to the individual.
- **Sensitive Personally Identifiable Information (SPII)**. A subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual. At EPA, SPII is defined as social security numbers or comparable identification numbers, biometric data, financial information or medical information associated with an individual. SPII requires additional levels of security controls.

Abbreviations including acronyms are summarized in *Appendix: Acronyms & Abbreviations*.

10. WAIVERS

Waivers for maintaining records offsite longer than ninety (90) days must be submitted to and approved by the SIO.

11. MATERIAL SUPERSEDED

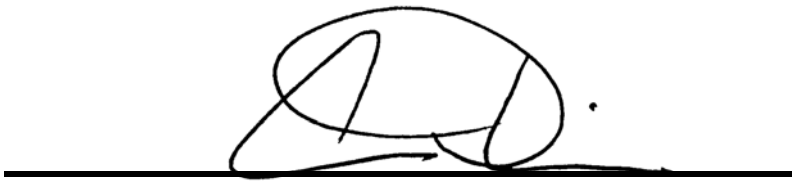
CIO Policy Transmittal 06-11: Interim Policy and Procedures for Protecting Personally Identifiable Information (PII) – June 23, 2006

Protecting Sensitive Personally Identifiable Information (SPII)		
Directive No.: 2151-P-10.0	CIO Approval: 12/19/2016	Transmittal No.: 17-001

CIO Policy Transmittal 01-09: Interim Procedures for Transmitting and Transporting Sensitive Personally Identifiable Information (PII) – January 16, 2009

12. CONTACTS

For further information, please contact the Office of Environmental Information, Office of Information Security & Privacy, Agency Privacy Officer.



Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

Protecting Sensitive Personally Identifiable Information (SPII)		
Directive No.: 2151-P-10.0	CIO Approval: 12/19/2016	Transmittal No.: 17-001

APPENDIX:
ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IMO	Information Management Officer
ISO	Information Security Officer
IT	Information Technology
MOU	Memorandum of Understanding
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
SIO	Senior Information Official
SO	System Owner
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number