Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Personally Identifiable Information Processing and Transparency (PT) Procedures

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Personally Identifiable Information (PII) Processing and Transparency (PT) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE

These procedures address all United States Environmental Protection Agency (EPA) information and information systems to include information and information systems used, managed, or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO), Liaison Privacy Official (LPO), and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

EPA is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems shall meet security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the PII Processing and Transparency Procedures include:

- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- E-Government Act of 2002, Section 208, 44 U.S.C. 3501
- Privacy Act of 1974 (5 U.S.C. § 552a) as amended
- OMB Circular A-130, “Managing Information as a Strategic Resource,” July 2016
- OMB Circular A-108, “Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,” December 2016
- Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503), October 1988
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Controlled Unclassified Information (CUI) Policy
- EPA Controlled Unclassified Information (CUI) Procedure

6. PROCEDURE

SIO, ISO, LPO, and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system though a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO, and EPA SO or their official designees and SM for the systems that they oversee.

The "PT" designator (e.g., PT-2, PT-3) identified for each procedure below corresponds to the NIST- identifier for the Personally Identifiable Information Processing and Transparency control family, as identified in NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

The PT controls are not allocated to the security control baselines, rather they are allocated to the privacy control baseline in accordance with NIST 800-53B, “Control Baselines for Information Systems and Organizations.”

PT-2 – Authority to Process Personally Identifiable Information

1) Determine and document the legal authority that permits the collection, use, maintenance and sharing either generally or in support of a specific program or information system of personally identifiable information; and
2) Restrict the collection, use, maintenance, sharing, storage, and processing of personally identifiable information to only that which is authorized.

PT-3 – Personally Identifiable Information Processing Purposes

1) Identify and document the purposes for collecting, using, maintenance, storing, sharing, or other purposes for processing personally identifiable information;
2) Describe the purpose(s) in the public privacy notices and policies of the organization;
3) Restrict the collection, use, maintenance, storing, sharing or other processing of personally identifiable information to only that which is compatible with the identified purpose(s); and
4) Monitor changes in processing personally identifiable information and implement mechanisms which may include (but are not limited to), obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information (PII) processing purposes to ensure that any changes are made in accordance with EPA requirements for safeguarding PII and Privacy Act information.

PT-4 – Consent

1) Implement automated mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

PT-5 – Privacy Notice

1) Provide notice to individuals about the processing of personally identifiable information that:
   a) Is available to individuals upon first interacting with an organization, and subsequently at the direction of the Agency Privacy Officer (APO) and legal counsel;
   b) Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
   c) Identifies the authority that authorizes the processing of personally identifiable information;
   d) Identifies the purposes for which personally identifiable information is to be processed; and
   e) Includes external parties with whom the information may be shared; whether disclosure of such information is mandatory or voluntary; and the effects on them, if any, of not providing any or all of the requested information.

PT-5(2) – Privacy Notice | Privacy Act Statements

1) Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

PT-6 – System of Record Notice

1) For systems that process information that will be maintained in a Privacy Act system of records:
   a) Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
   b) Publish system of records notices in the Federal Register; and
   c) Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

PT-6(1) – System of Records Notice | Routine Uses

1) Review all routine uses published in the system of records notice annually or when the purposes or information stated in the system of records notice has changed to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

PT-6(2) – System of Records Notice | Exemption Rules

1) Review all Privacy Act exemptions claimed for the system of records annually or when the purposes or information stated in the system of records notice has changed to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

PT-7 – Specific Categories of Personally Identifiable Information

1) Apply, at a minimum, the least privilege concept (i.e., need to know, proper authorization), and deploy protections such as encryption based on the sensitivity for specific categories of personally identifiable information.

PT-7(1) – Specific Categories of Personally Identifiable Information | Social Security Numbers

1) When a system processes Social Security numbers:

a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

PT-7(2) – Specific Categories of Personally Identifiable Information | First Amendment Information

1) Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

PT-8 – Computer Matching Requirements

1) When a system or organization processes information for the purpose of conducting a matching program:
   a) Obtain approval from the Data Integrity Board to conduct the matching program;
   b) Develop and enter into a computer matching agreement;
   c) Publish a matching notice in the Federal Register;
   d) Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
   e) Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMATION

The information listed below relates to the PII Processing and Transparency Procedures.

- NIST Special Publications, 800 series
- The National Strategy to Secure Cyberspace, February 2003
- EPA Information Security – Privacy Procedure Documents

9. DEFINITIONS

Definitions which pertain to the PII Processing and Transparency Procedures are listed below.

- **Computer Matching Program** – The comparison of automated records using a computer. Manual comparisons of printouts of two automated data bases are not included in this definition. A matching program covers the actual computerized comparison and any investigative follow-up and ultimate action. Public Law 100-503 divides computer matching programs into covered and non-covered matching programs. Two kinds of matching programs are covered: (1) matches involving federal benefits programs, and (2) matches using records from federal personnel or payroll systems of records. Questions concerning whether a match is covered by the CMPPA should be referred to the Agency Privacy Officer.
- Controlled Unclassified Information (CUI) – Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
- **Information Security** – the practice of defending information from unauthorized access, use, disclosure, disruption, modification, or destruction, usually by enacting security controls.
- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an Agency, which can be used to distinguish, trace or identify the individual, including personal information which is linked or linkable to that individual. PII may be classified into sensitive and non-sensitive.
- **Plan of Action and Milestones (POA&M)** – plans of corrective actions that are designed to counter discovered risks and threats to the organization or organizational assets.
- **Risk** – the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **Risk Assessment** – the process of identifying risks to Agency operations (including mission, functions, image or reputation), Agency assets, individuals, other organizations and the Nation arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.
- **Sensitive Personally Identifiable Information (SPII)** - Social Security numbers or comparable (e.g., biometrics and passport number), or financial and medical information associated with individuals. Sensitive PII is a subset of PII and requires additional levels of security controls.

- **System of Records** – A group of any records, paper or electronic, under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying assigned to the individual.

10. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

N/A

12. CONTACTS

For further information, please contact the Office of Mission Support (OMS) or the Office of Information Security and Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.09.05 09:45:19 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS AND ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
OTOP	Office of Technology Operations and Planning
PII	Personally Identifiable Information
PO/R	Program Office/Region
POA&M	Plan of Action and Milestones
PT	Processing and Transparency
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
U.S.C.	United States Code