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

Information Security – Privacy Procedures

1. PURPOSE

To implement the security control requirements for the Privacy Control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

2. SCOPE

The procedures cover all 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.

The procedures apply to all EPA employees, contractors and all other users of EPA information and information systems that support the operation and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the 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 the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The document addresses the procedures and standards set forth by the EPA and complies with the family of Privacy Controls.

Per OMB M-06-19 (July 12, 2006), "The term Personally Identifiable Information (PII) means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.”

Sensitive Personally Identifiable Information (SPII) is a subset of PII, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. The EPA defines SPII as Social Security numbers or comparable identification numbers, biometrics, financial information associated with individuals, and medical information associated with individuals. SPII requires additional levels of security controls. The Privacy Act only protects personal information that is contained in a Privacy Act System of Records. A Privacy Act System of Records Notice (SORN) must be published in the Congressional Record prior to activation of a SOR containing Privacy Act Information. To protect PII, users shall comply with the EPA's Privacy Policy and other related procedures.

5. AUTHORITY

- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C— "Employees Responsible for the Management or Use of Federal Computer Systems," Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-00-07, "Incorporating and Funding Security in Information Systems Investments," February 2000
- OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 2003
- OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," June 2006
- OMB Circular A-11, "Preparation, Submission and Execution of the Budget," June 2006
- OMB Circular A-123, "Revisions to OMB Circular A-123, Management's Responsibility for Internal Control," December 2004
- OMB Circular A-130, "Management of Federal Information Resources," July 2016
- Federal Information Processing Standards (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
- Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- Federal Information Processing Standards (FIPS) 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy

- EPA Privacy Policy
- EPA Roles and Responsibilities Procedures
- CIO Policy Framework and Numbering System
- EPA 2151.0 Information Privacy Policy

6. PROCEDURE

For the following section titles, the "AP," "AR," etc., designators identified in each procedure represents the NIST-specified identifiers for the Privacy *control family* and the number associated with the control family (e.g., "AP-1") represents the *control identifier*, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

A list of abbreviations including acronyms is provided in the Appendix.

AP-1 AUTHORITY TO COLLECT

1) System Owners (SO) in coordination with Information Management Officers (IMO) and Information Owners (IO) for EPA-operated systems shall; and Service Managers (SM), in coordination with IOs and IMOs for systems operated on behalf of the EPA, shall ensure that service providers:

   a) Determine and document[1] the legal authority that permits the collection, use, maintenance and sharing of PII, either generally or in support of a specific program or information system.

      i) The SO shall remain responsible for identification and collection of PII within their respective systems.

   b) Inform the National Privacy Program of any documentation that shares PII derived from Federal information systems.

AP-2 Purpose Specification

1) IMOs in coordination with the Director of the Office of Information Security and Privacy (OISP) and Chief Privacy Officer (CPO) (OISP-CPO) shall:

   a) Describe the purpose(s)[2] for which PII is collected, used, maintained and shared in its privacy notices and agreements.

AR-1 GOVERNANCE AND PRIVACY PROGRAM

1) The CIO shall:
   a) Act as the Senior Agency Official for Privacy (SAOP), accountable for developing,

[1] *NIST SP 800-53, Rev 4 states, "The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements."*

[2] *NIST SP 800-53, Rev 4 states "Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII)."*

implementing and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing and disposal of PII by programs and information systems;

b) Allocate sufficient staff and funding to implement and operate the organization-wide privacy program;
   i) The OISP-CPO shall submit staff and budget proposals to the CIO annually and inform the CIO of program requirements;
c) Develop a strategic plan for implementing applicable privacy controls, policies and procedures; and
d) Implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

2) The Agency Privacy Officer shall:
   a) Monitor federal privacy laws and policies for changes that affect the privacy program;
   b) Develop and disseminate operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems or technologies involving PII; and
   c) Review and update the privacy plan, policies, and procedures annually, as required.

AR-2 PRIVACY IMPACT AND RISK ASSESSMENT

1) The Agency Privacy Officer shall:
   a) Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use and disposal of PII; and
   b) In accordance with applicable law, OMB policy or any existing organizational policies and procedures, conduct oversight of the Privacy Impact Assessment (PIA) process for information systems, programs, or other activities that pose a privacy risk.

AR-3 PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

1) The OISP-CPO and the Agency Privacy Officer shall establish privacy roles, responsibilities and access requirements for contractors and service providers;
2) The Director of the OMS Office of Acquisition Solutions (OAS) shall include privacy requirements in contracts and other acquisition-related documents and report conformance to requirements to the National Privacy Program annually; and
3) OISP Chief Privacy Officer (CPO) shall provide OAM with a list of Privacy Act System of Records Notices (SORN) to identify systems that require contract clauses.

AR-4 PRIVACY MONITORING AND AUDITING

1) The Director of OISP, shall monitor and audit privacy controls and internal privacy policy on a continuous basis to ensure effective implementation of this procedure.

AR-5 PRIVACY AWARENESS AND TRAINING

1) The OISP-CPO and the Agency Privacy Officer, in coordination with the Office of Mission Support-ARM, Office of Human Resources, and the Chief Information Security Officer (CISO) shall:

a) Develop, implement, and maintain a comprehensive training and awareness strategy to ensure that personnel understand privacy responsibilities and procedures;

b) Annually administer basic privacy training to all personnel and role-based privacy training for key (or identified) personnel responsible for PII; and

c) Annually ensure that personnel certify (manually or electronically) acceptance of responsibility for privacy requirements.

AR-6 PRIVACY REPORTING

1) The Agency Privacy Officer shall develop, disseminate and update reports to the OMB, Congress and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

AR-7 PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT

1) IOs, in coordination with SOs, shall:

   a) Support privacy by automating privacy controls; and

   b) Ensure SPII is adequately protected through cryptographic mechanisms and security controls.

AR-8 Accounting of Disclosures

1) The OISP-CPO and the Agency Privacy Officer, in coordination with IOs and SOs, shall:

   a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including:

      i) Date, nature and purpose of each disclosure of a record; and

      ii) Name and address of the person or agency to which the disclosure was made;

   b) Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

   c) Make the accounting of disclosures available to the person named in the record upon request.

DI-1 Data Quality

1) The Agency Privacy Officer, in coordination with IOs and SOs, shall:

   a) Confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;

   b) Collect PII directly from the individual to the greatest extent practicable (i.e., when a known data source is not available);

   c) Check for, and correct as necessary, any inaccurate or outdated PII used by the Agency's programs or systems quarterly; and

   d) Issue guidelines that maximize the quality, utility, objectivity, and integrity of disseminated information.

DI-2 Data Integrity and Data Integrity Board

1) The CIO shall:
   a) Document processes to ensure the integrity of PII through existing security controls; and
   b) When appropriate, establish a Data Integrity Board to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Computer Matching and Privacy Protection Act (CMPPA).

DM-1 Minimization of Personally Identifiable Information

1) The OISP-CPO and Senior Information Officials (SIO) shall:
   a) Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
   b) Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent;
   c) Conduct an initial evaluation of PII holdings; and
   d) Establish and follow a schedule for reviewing PII holdings annually to ensure that only PII identified in the systems is collected and retained in accordance with Agency procedures and that the PII continues to be necessary to accomplish the legally authorized purpose.

DM-2 Data Retention and Disposal

1) SOs and IOs shall:
   (a) Retain each collection of PII for the period identified in NARA record retention schedules to fulfill the purpose(s) identified in the notice or as required by law;
   (b) Dispose of, destroy, erase and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
   (c) Use techniques identified in NIST SP 800-88, Guidelines for Media Sanitization, to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

DM-3 Minimization of PII Used in Testing, Training, and Research

1) The OISP-CPO and the Agency Privacy Officer shall develop policy and procedures that:
   a) Minimize the use of PII for testing, training and research; and
   b) Implement controls to protect PII used for testing, training and research.

IP-1 Consent

1) SOs with support from the OISP-CPO and the Agency Privacy Officer shall:
   a) Provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection;
   b) Provide appropriate means for individuals to understand the consequences of the decision to decline the collection, use, dissemination and retention of PII;
   c) Obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d) Ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice.

IP-2 Individual Access

1) SOs with support from the OISP-CPO and the Agency Privacy Officer shall:
   a) Provide individuals the ability to access their PII maintained in its system(s) of records;
   b) Publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
   c) Publish access procedures in SORNs; and
   d) Adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

IP-3 Redress

1) The Agency Privacy Officer, in coordination with the SO shall:
   a) Provide a process for individuals to request that inaccurate PII maintained by the organization corrected or amended, as appropriate; and
   b) Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended.

IP-4 Complaint Management

1) The OISP-CPO and the Agency Privacy Officer shall:
   a) Implement a process to receive and respond to complaints, concerns, or questions from individuals about the organizational privacy practices.

SE-1 Inventory of Personally Identifiable Information

1) SOs with support from the OISP-CPO and the Agency Privacy Officer shall:
   a) Establish, maintain, and update on an annual basis an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining or sharing PII; and
   b) Provide each update of the PII inventory to the CIO annually to support the establishment of information security requirements for all new or modified information systems containing PII.

SE-2 Privacy Incident Response

1) OISP and shall:
   a) Develop and implement a Privacy Incident Response Plan; and
   b) Provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Handling Plan and CIO-2151-P-02.2, EPA Procedure for Responding to Breaches of Personally Identifiable Information (PII).[3]

[3] *CIO-2151-P-02.4, EPA Procedure for Responding to Breaches of Personally Identifiable Information (PII) is located at https://www.epa.gov/sites/production/files/2020-02/documents/responding_to_personally_identifiable_information_pii_breach_procedure_20190820_508_vwn.pdf*

TR-1 Privacy Notice

1) The OISP-CPO, the Agency Privacy Officer and the SO shall:
   a) Provide effective notice via the Privacy Act Statement (PAS) to the public and to individuals regarding:
      i) Its activities that impact privacy including its collection, use, sharing, safeguarding, maintenance and disposal of PII;
      ii) Authority for collecting PII;
      iii) The choices individuals may have regarding how the organization uses and shares PII; and
      iv) The consequences of not supplying information, if SSN is requested.
   b) Describe:
      i) The PII the organization collects and the purpose(s) for which it collects that information;
      ii) How the organization uses PII;
      iii) Whether the organization shares PII with external entities and the purposes for such sharing;
      iv) Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
      v) How individuals may obtain access to PII; and
      vi) How the PII will be protected;
   c) Revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy before or as soon as practicable after the change.

TR-2 System of Records Notices and Privacy Act Statements

1) The OISP-CPO, the Agency Privacy Officer and the SO shall:
   a) Publish SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;
   b) Keep SORNs current; and
   c) Include Privacy Act Statements on Agency forms that collect PII, or on separate forms that can be retained by individuals, to provide notice to individuals from whom the information is being collected.

TR-3 Dissemination of Privacy Program Information

1) The OISP-CPO and the Agency Privacy Officer shall:
   a) Ensure that the public has access to information about its privacy activities and is able to communicate with its SAOP; and
   b) Ensure that its privacy practices are publicly available through organizational websites or otherwise.

UL-1 Internal Use

The OISP-CPO, the Agency Privacy Officer and SO shall ensure that the usage of PII internally is only for the authorized purpose(s) identified in the Privacy Act and/or Federal Information Systems (FIS).

UL-2 Information Sharing with Third Parties

1) The SO, OISP-CPO and the Agency Privacy Officer shall:
   a) Share PII externally, only for the authorized purposes identified in the Privacy Act, as described in its notice(s), and for a use that is compatible with those collections;
   b) Where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements or similar agreements with third parties that specifically describe the PII covered and enumerate the purposes for which the shared or distributed PII may be used;
   c) Monitor, audit and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
   d) Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

7. ROLES AND RESPONSIBILITIES

Agency Privacy Officer

1) The Agency Privacy Officer has the following responsibilities with respect to privacy:
   a) Develop Agency level privacy policies, procedures, standards and guidelines, as needed;
   b) Develop accountability guidance which identifies positions/job types with key Privacy Program responsibilities and appropriate sample cascading goals and objectives that managers can use to establish accountability within their respective offices;
   c) Provide overall privacy management and policy guidance;
   d) Provide oversight of system managers' activities to ensure all privacy-related, statutory, regulatory and EPA requirements are met;
   e) Implement changes in a timely manner to Agency level privacy policies, procedures, standards, and guidelines. Change is based on the results of the Agency Privacy Officer's oversight of system managers' activities, the monitoring and oversight results reported by Liaison Privacy Officials (LPO), as well as updates from OMB, changes in regulations, changes in roles and responsibilities, etc.;
   f) Develops and implements response procedures to be followed in the event of a breach of PII and SPII;
   g) Coordinate privacy-related activities and responses to breaches of PII and SPII with Agency managers as appropriate;
   h) Publish Federal Register notices for systems of records as required by the Privacy Act;
   i) Review privacy impact assessments as required by the E-Government Act;
   j) Establish the network of LPOs;
   k) Develop and implements an annual LPO awareness training program;
   l) Advise and trains system managers and other EPA personnel on privacy requirements;
   m) Monitor EPA privacy activities, including quality and timeliness of responses to Privacy Act requests;
   n) Transmit letters to Congress and OMB;
   o) Compile a biennial report on the computer matching activities and submit to OMB;

p) Report privacy data specified by OMB annually on the FISMA Report to OMB; and
q) Review and approves PII elements on forms prior to number issuance.

Chief Information Officer (CIO) is the designated **Senior Agency Official for Privacy (SAOP)** in accordance with the E-Government Act

1) The SAOP has overall responsibility and accountability for ensuring the Agency's implementation of information privacy protections, including the agency's full compliance with Federal laws, regulations and policies relating to information privacy, such as the Privacy Act and E-Government Act; and
   a) Designates the Privacy Officer;
   b) Approves Agency level privacy policies, procedures, standards and guidelines;
   c) Approves the establishment or amendment of EPA Privacy Act Systems of Records Notices according to the Administrator's delegation;
   d) Ensures that appropriate changes are made in a timely manner to privacy policies, procedures, standards and guidelines based on the oversight results reported by the Office of Information Collection as well as updates from OMB, changes in regulations, changes in roles and responsibilities, etc.;
   e) Convenes the Data Integrity Board (DIB) to carry out computer matching responsibilities pursuant to the Computer Matching Privacy Protection Act (CMPPA);
   f) Ensures that accountability guidance, which identifies positions/job types with key Privacy Program responsibilities and appropriate sample cascading goals and objectives that managers can use to establish accountability within their respective offices, are developed and communicated;
   g) Ensures the Agency conducts periodic reviews to promptly identify deficiencies, weaknesses or risks;
   h) Participates in assessing the impact of technology on the privacy of personal information;
   i) Ensures that the Agency takes appropriate steps to remedy compliance issues identified;
   j) Acts as the Chair for the Breach Notification Team (BNT) as required by M-07-16; and
   k) Chairs and convenes the DIB to carry out computer matching responsibilities pursuant to the Computer Matching and Privacy Protection Act (CMPPA) of 1988.

Information Management Officer (IMO)

1) IMOs have the following responsibilities with respect to privacy:
   a) Identify and collect PII within their perspective systems, in coordination with the System Owner and Information Owners;
   b) Describe the purpose(s) for which PII is collected, used, maintained and shared in its privacy notices, in coordination with the Director of OISP;
   c) Respond to data calls issued by NPP; and
   d) Periodically review existing databases containing PII to determine if data elements are still required.

Information Owners (IO)

1) IOs have the following responsibilities with respect to privacy:
   a) Identify and collect PII within their perspective systems, in coordination with the System Owner and Information Management Officer;
   b) Describe the purpose(s) for which PII is collected, used, maintained and shared in its privacy notices, in coordination with the Director of OISP;
   c) Retain collection of PII for timelines identified in NARA record retention schedules to fulfill the purpose(s) identified in the notice or as required by law;
   d) Dispose of, destroy, erase and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse or unauthorized access;
   e) Use techniques identified in NIST Special Publication 800-88, Guidelines for Media Sanitization to ensure secure deletion or destruction of PII (including originals, copies and archived records);
   f) Ensure terms of service and other contractual agreements satisfy the security and privacy requirements applicable to EPA information systems and information for services for non- enterprise services obtained; and
   g) Respond to data calls issued by the NPP.

Liaison Privacy Officials (LPOs), designated by the SIO

1) LPOs have the following responsibilities with respect to privacy:
   a) Administer the day-to-day activities and responsibilities of privacy in their specific program and regional areas;
   b) Ensure proper training for individuals in their area of responsibility, including monitoring on-line training for the employees;
   c) Attend annual training for LPOs; and
   d) Ensure Agency inventory of federally identifiable systems are up-to-date.

Office of Mission Support (OMS) Office of Acquisition Solutions (OAS)

1) OAS has the following responsibilities with respect to privacy:
   a) Ensure appropriate privacy related language is included in contracts, grants and interagency agreements; and
   b) Review and approve sample privacy cascading goals and objectives developed by OARM to use to establish accountability within their respective offices; and
   c) Report on Electronic Official Personnel Folder (EOPF) misfiles.

Office of Public Affairs (OPA) in the Administrator's Office

1) OPA has the following responsibilities with respect to privacy:
   a) Post Privacy and Security Notices on all EPA public access website pages, EPA printed publications and other EPA information media; and
   b) Participate in the response to breaches of PII as appropriate.

Office of Information Management (OIM) in Office of Mission Support (OMS)

1) OIM has the following responsibilities with respect to privacy:
   a) Maintain and update the Privacy and Security Notices, which are posted on all EPA public access websites. Content on the Privacy and Security Notice is coordinated with OPA and the Agency Privacy Officer.

Office of Information Security and Privacy (OISP) in OMS-EI

1) OISP is responsible for implementing the Privacy Program at EPA. In this capacity, OISP:
   a) Establishes key goals and objectives associated with the Agency's Privacy Program;
   b) Establishes and tracks performance measures associated with the key goals and activities associated with the Agency's Privacy Program and measures the progress of the Privacy Program;
   c) Establishes performance measurement report(s) for tracking the Agency's Privacy Program progress;
   d) Provides annual performance measurement reports showing the progress of the Agency's Privacy Program to the Senior Agency Official for Privacy and makes the reports available to the EPA offices and regions responsible for implementing the Privacy Program;
   e) Reviews/approves Privacy Impact Assessments in accordance with Provisions of Section 208 of the E-Government Act of 2002;
   f) Leads Agency efforts to protect PII used for Agency operations;
   g) Performs oversight of the implementation of the Agency level privacy policies, procedures, standards and guidelines within the Program and Regional Offices to ensure they are properly executed, consistently applied and effective;
   h) Reports the oversight results to the Senior Agency Official for Privacy, the Agency's Assistant and Regional Administrators and the Agency's Senior Information Officers;
   i) Reports annually on the implementation of the Privacy Act within the FISMA report;
   j) Monitors the content of the Privacy website and EPA printed publications to ensure that non-public information about EPA employees is protected from public view; and
   k) Manages the network of Liaison Privacy Officials.

Office of Information Technology Operations (OITO) in OMS-EI

1) OITO has the following responsibilities with respect to privacy:
   a) Support privacy policies through its planning, operational, training and oversight responsibilities for IT;
   b) Assist in recommending and developing appropriate technical solutions to protect the privacy information collected or maintained within IT systems; and
   c) Support activities in response to breaches of PII.

Office of the General Counsel (OGC)

1) OGC has the following responsibilities with respect to privacy:
   a) Interpret the Privacy Act and other privacy-related regulations, statutes and requirements;
   b) Review related privacy notices, regulations and policy statements for legal form and substance;
   c) Decide on written appeals from initial denials of Privacy Act information to an individual, including denial of a request for correction or amendment of a record

pursuant to the Privacy Act, 5 U.552a, as stated within EPA Delegation 1-33;

d) Participate in computer matching programs as required (http://www.dhs.gov/computer-matching-programs); and

e) Participate in Agency responses to breaches of PII, as appropriate.

Office of the Inspector General (OIG)

1) OIG has the following responsibilities with respect to privacy:

a) Carry out the appeal responsibilities related to decisions made on OIG Privacy Act records;

b) Participate in computer matching programs as required; and

c) Conduct criminal investigations related to a breach of SPII or disclosure of PII if circumstances warrant such an investigation.

Senior Information Officials (SIOs)

1) SIOs have the following responsibilities with respect to privacy:

a) Provide oversight, coordination and management of information technology used in fulfilling their organization's business needs and mission;

b) Establish appropriate policies and procedures within their respective offices to implement the Agency level policies, procedures, standards and guidelines;

c) Monitor and perform oversight of the implementation of the program or regional privacy policies and procedures to ensure they are properly executed, consistently applied and effective;

d) Make appropriate changes in a timely manner to program or regional privacy policies and procedures based on the monitoring and oversight results, and recommend changes to Agency level policies and procedures as appropriate;

e) Ensure guidance which identifies positions/job types with key Privacy Program responsibilities along with appropriate sample cascading goals and objectives is applied within their respective offices as well as including Critical Job Elements in the PARS;

f) Designate the LPOs;

g) Ensure that a PIA has been completed prior to establishing a new or significantly modified collection of Privacy related information;

h) Review and make written determinations concerning all requests to access SPII from a remote location or take SPII off site;

i) Ensure compliance with federal regulations and Agency policies and procedures for protecting data in mobile devices is used to transport or access PII;

j) Maintain a documented record of all approved remote access, transport of SPII, downloads and/or local storage on a computer not located within EPA space;

k) Ensure all copies of SPII approved to be stored off site are erased or returned within 90 days; and

l) Ensure coordination with Agency managers including, but not limited to, Assistant Administrators, Chief Financial Officer, Chief Information Officer, Director of OITO, Chief Information Security Officer, Computer Security Incident Response Center, Office of Inspector General, OPA, and Office of General Counsel in response to a breach of SPII.

System Owners in Program Offices and Regional Offices

1) System Owners have the following responsibilities with respect to privacy:
   a) Apply privacy requirements, policies, procedures, and guidance to Privacy Act systems of records and systems subject to the E-Gov Act and other privacy related systems. Specifically, System Owners:
      i) Establish safeguards to ensure Confidentiality Integrity and Availability (CIA);
      ii) Authorize privacy documentation for new and/or revised systems;
      iii) Terminate systems when no longer maintained in accordance with proper destruction/transfer procedures;
      iv) Approve initial determinations on access to information in an FIS;
      v) Account for access, amendments and disclosures from Privacy Act System of Record;
      vi) Recommend the designation of an LPO;
      vii) Ensure that a Privacy Threshold Analysis is conducted for newly developed systems and/or systems that undergo substantial revisions; and
      viii) Ensure completion of a PIA for any system that undergoes substantial revisions or that collects PII or SPII.

8. RELATED INFORMATION

NIST Special Publications, 800 series
Related policy and procedures are available on the OMS Policy Resources website.
https://www.epa.gov/irmpoli8/current-information-directives
Related standards and guidelines are available on the OMS website.
http://intranet.epa.gov/privacy/

9. DEFINITIONS

- **Assessment** – See Security Control Assessment.
- **Authorization** – the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
- **Availability** – ensuring timely and reliable access to, and use of, information.
- **Compensating Control** – a management, operational or technical control employed by an information system in lieu of a recommended security control in the low, moderate or high baselines described in NIST SP 800-53 (as amended), which provides equivalent or comparable protection for an information system.
- **Confidentiality** – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Information** – an instance of an information type.
- **Information Security** – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Information System** – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- **Information Technology (IT)** – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- **Integrity** – guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.
- **Organization** – a federal agency or, as appropriate, any of its operational elements.
- **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.
- **Privacy Impact Assessment (PIA)** – an analysis of how information is handled (i) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
- **Scoping Guidance** – provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.
- **Security Control Assessment** – the testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.
- **Security Requirements** – requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures or organizational mission/business case needs to ensure the confidentiality, integrity and availability of the information being processed, stored or transmitted.
- **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. The EPA defines SPII as social security numbers or comparable identification numbers, financial information associated with individuals, and medical information associated with individuals. SPII requires additional levels of security controls.

- **Signature (of an individual)** – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation (can be accomplished manually, sometimes referred to as a "wet signature," or electronically).
- **Significant Change** – a modification that impacts the operating environment, functional design, operation, or protective controls required for a system. Changes in user audiences, owning organization, public access and communication methods are considered significant changes. Other examples of a significant change include, but are not limited to, a change in criticality and/or sensitivity level that causes a change in the controls or countermeasures required; a change in the security policy; a change in the threat of system risk; a change in the activity that requires a different mode of operation; additions or a change to the operating system or to software providing security features; additions or a change to the hardware that requires a change in the approved security countermeasures; a breach of security, a breach of system integrity or an unusual situation that appears to be a breach; a significant change to the physical structure of the facility or to the operating procedures; a move to another location; and a significant change to the configuration of the system.
- **System Security Plan (SSP)** – a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
- **User** – individual or (system) process authorized to access an information system.
- **Written (or in writing***)* – to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The CISO and Director, OITO shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition, Sections 2.6.1, and 13.0

12. CONTACTS

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

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2020.11.13 10:06:49 -05'00'

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

APPENDIX: ACRONYMS AND ABBREVIATIONS

AO	Authorizing Official
CIA	Confidentiality, Availability, Integrity
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMPPA	Computer Matching and Privacy Protection Act
CPO	Chief Privacy Officer
BNT	Breach Notification Team
DIB	Data Integrity Board
EFOIA	Electronic Freedom of Information Act: E-FOIA (see January 21, 2009 Presidential Memo on Freedom of Information Act)
EPA	Environmental Protection Agency
EOPF	Electronic Official Personnel Folder
FIPS	Federal Information Processing Standards
FIS	Federal Information System
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act (2002)
FISMA	Federal Information Security Modernization Act (2014)
FOIA	Freedom of Information Act
GAO	Government Accountability Office
IG	Inspector General
IO	Information Owner / Steward
IMO	Information Management Officer
ISA	Interconnection Security Agreement
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
JFMIP	Joint Financial Management Improvement Program
LPO	Liaison Privacy Official
MISD	Mission Investment Solutions Division
MOU/A	Memorandum of Understanding or Agreement
NPP	National Privacy Program
NROB	National Rules of Behavior
NIST	National Institute of Standards and Technology
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIM	Office of Information Management
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
OMS	Office of Mission Support
OPA	Office of Public Affairs within the Office of the Administrator
PAS	Privacy Act Statement
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SA&A	Security Assessment and Authorization

SAOP	Senior Agency Official for Privacy
SCA	Security Controls Assessment
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SSP	System Security Plan
USC	United States Code