

SUPPLEMENTAL DIRECTIVE

NNSA SD 206.1

Approved: 06-22-18

Expires: 06-22-21

PRIVACY PROGRAM



NATIONAL NUCLEAR SECURITY ADMINISTRATION Office of Information Management

CONTROLLED DOCUMENT

AVAILABLE ON-LINE AT:

<https://nnsa.energy.gov/aboutus/ouoperations/managementandbudget/policysystem>

OFFICE OF PRIMARY INTEREST (OPI):

Office of Information Management

printed copies are uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

PRIVACY PROGRAM

1. **PURPOSE.** To set forth supplemental requirements to Department of Energy (DOE) Order (O) 206.1, *DOE Privacy Program*, by establishing a privacy program within the National Nuclear Security Administration (NNSA) and appointing the roles of the Chief Privacy Officer (CPO) and the NNSA Privacy Act Officer (PAO), who will be responsible for managing the Privacy Program. This Supplemental Directive (SD) ensures NNSA meets federal guidelines regarding privacy and has an effective information privacy program.
2. **CANCELLATIONS.** None.
3. **APPLICABILITY.**
 - a. **Federal.** This SD applies to all NNSA federal personnel who handle, collect, control, maintain, or access documents, records, federal information, information technology, or information systems that contain or store *Privacy Act* information and Personally Identifiable Information (PII) for NNSA.
 - b. **Contractors.** The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this policy that apply to site and facility management contractors whose contracts include this CRD. The CRD, and all applicable attachments, must be included in site and facility management contracts where contractors handle, control, maintain, access, or disseminate documents, records, or manage federal information, information technology, or information systems that contain or store *Privacy Act* information and PII for NNSA.
 - c. **Equivalency.** In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 United States Code (U.S.C.) sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.
4. **SUMMARY OF CHANGES.** Not applicable.
5. **BACKGROUND.** This SD was developed using DOE O 206.1 as a baseline, and is tailored to meet the mission requirements of NNSA. This SD incorporates and requires a privacy program consistent with federal policies, instructions, standards, and guidelines, and supports the direction from the *Privacy Act*.

6. REQUIREMENTS.

- a. NNSA must establish and maintain a privacy program that provides oversight for administering and ensuring NNSA's compliance with Federal Regulations and DOE requirements in regard to *Privacy Act* information, PII protection, and privacy management. The NNSA Privacy Program must:
- (1) Comply with the plans, controls, and assessments responsibilities per OMB Circular A-130, Appendix II, *Responsibilities for Managing Personally Identifiable Information*, and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.
 - (2) Require compliance with the *Privacy Act* and Privacy Impact Assessments (PIAs) guidance. NNSA PIAs are to be completed on Form 206.1 <https://www.energy.gov/cio/downloads/doi-f-2061>. NNSA SD Form 206.1 must be completed and signed by the NNSA CPO for NNSA PIAs. A copy of the form can be found in Attachment 2.
 - (3) Implement the requirements and safeguards identified in DOE O 206.1.
- b. NNSA must:
- (1) Define the roles and responsibilities required to implement the NNSA Privacy Program requirements in accordance with DOE O 206.1.
 - (2) Appoint a CPO with NNSA-wide accountability for information privacy issues.
 - (3) Appoint an NNSA PAO responsible for managing the NNSA Privacy Program, per DOE O 206.1.
 - (4) Appoint a Privacy Representative at each NNSA Element who will provide oversight at their respective program or site.
 - (5) Establish processes to ensure all NNSA employees complete privacy training that includes the management of PII.
- c. Social security numbers must only be collected for the performance of the program's or office's work, or to perform an agency function, and as authorized.
- d. PII and *Privacy Act* information, in any format, electronic or hard copy, must be protected and secured, and disposed of when no longer required in accordance to records disposition schedules.

7. RESPONSIBILITIES.

a. Associate Administrator for Information Management and Chief Information Officer (CIO).

- (1) Is accountable for the NNSA Privacy Program.
- (2) Serves as the NNSA Chief Privacy Officer. This role can be delegated as needed.
- (3) Promotes Privacy Program awareness, requirements, and expectations to NNSA Executives and Senior Leadership.

b. NNSA Chief Privacy Officer (CPO).

- (1) Oversees, coordinates, and facilitates the NNSA Privacy Program by ensuring the program is in full compliance with federal laws, regulations, and policies relating to information privacy.
- (2) Coordinates with the DOE Senior Agency Official for Privacy (SAOP) on department level privacy concerns and issues, which includes timely responses and reporting of privacy breaches, and implementing investigations and corrective actions.
- (3) Participates as a member in the agency's Privacy Incident Response Team.
- (4) Approves PIAs and System of Records Notices (SORNs) for NNSA.
- (5) Appoints the NNSA Privacy Act Officer who has the responsibility for managing the NNSA's Privacy Program.
- (6) Approves all NNSA policies and guidance developed and implemented by the NNSA PAO.
- (7) Identifies ways in which the NNSA can use technology to reinforce and sustain the privacy of personal information.

c. NNSA Privacy Act Officer (PAO).

- (1) Manages the NNSA Privacy Program as delegated by the CPO.
- (2) Coordinates with and supports the DOE SAOP on department level privacy activities to include PIA and SORN management, privacy training, annual incident response plan reviews, and managing PII incident management guidance.
- (3) Reviews and evaluates legislative, regulatory, and other policy proposals, which involve information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information.

- (4) Coordinates with Information Assurance Response Center (IARC) on notification of reported PII related incidents.
- (5) Develops privacy policy and training guidance for the proper handling of privacy information and the preparation of PIAs.
- (6) Advises NNSA elements, which includes the field offices, on the inclusion of privacy, confidentiality, and data security requirements in site level policies and programs.
- (7) Informs NNSA employees of their roles and responsibilities regarding privacy regulations and requirements.
- (8) Ensures PIAs are up to date and complete for all unclassified information systems within NNSA, including federal information systems that collect or maintain information about NNSA employees and contractors.
- (9) Ensures employees and contractors receive appropriate training and education on programs regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of privacy information.
- (10) In coordination with NNSA General Counsel, *Privacy and Freedom of Information Act* (FOIA) experts, ensures that NNSA provides a complete, legal, and prompt response to all individual requests for *Privacy Act* protected information, where appropriate.
- (11) Conducts a review of NNSA practices regarding collection or disclosure of personal information in privacy systems of records.
- (12) Provides mandatory reports on the status of NNSA privacy protections to DOE and the Office of Management and Budget (OMB).
- (13) Advises and provides guidance to appointed Privacy Representatives, with regard to conducting, writing, and completing the NNSA PIA and SORN process and privacy management.
- (14) Coordinates with NNSA General Counsel (NA-GC) regarding privacy matters, including policy requirements.
- (15) Ensures coordination between the privacy program and other programs, such as acquisitions and personnel, to ensure privacy is addressed throughout NNSA.

d. Program or Field Office Manager.

Appoints an NNSA Element Privacy Representative.

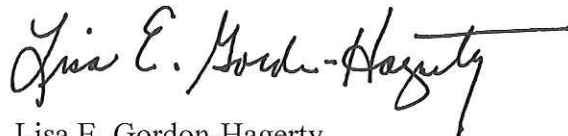
- e. NNSA Element Privacy Representative.
 - (1) Oversees local privacy development, implementation, and performance reporting activities at their respective program office or site.
 - (2) Participates in enterprise-wide privacy efforts.
 - (3) Involves NA-GC/Site Counsel in providing legal review, interpreting and applying privacy issues, including privacy law, compliance, and training.
 - (4) Serves as liaison for local privacy activities, to include completion of PIAs.

- f. NNSA Federal Employees.
 - (1) Ensure that PII and privacy information in any format is safeguarded and secured.
 - (2) Ensure proper handling of all information and information systems that contain PII.
 - (3) Complete annual privacy training provided by the agency.
 - (4) Report all *Privacy Act* violations and PII breaches to appropriate management officials as soon as possible.
 - (5) Cooperate with incident response teams that are investigating or attempting to resolve incidents involving PII.

- g. System Owners (Federal).
 - (1) Manage and monitor information systems under their purview to ensure compliance in accordance with OMB Circular A-130 and other applicable federal guidance and laws, and DOE O 206.1.
 - (2) Responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of privacy information including PII for their information system(s).
 - (3) Monitor their system to ensure that it is subject to a PIA and that the use of PII conforms to the use listed in the relevant SORN.
 - (4) In coordination with the NNSA Element Privacy Representative, review the site PIAs for conformance to requirements of DOE O 206.1, this SD, and SD 205.1, *Baseline Cybersecurity Program*.
 - (5) Determine, with the CPO, the appropriate allocation of resources dedicated to the protection of PII systems.

- h. NNSA General Counsel.
 - (1) Provides legal review and approval on all NNSA PIAs where the system contains PII, and reviews and approves applicable SORNs.
 - (2) Provides legal review and concurrence before an NNSA SORN is published in the Federal Register.
 - (3) Provides legal expertise to all NNSA elements in interpreting and applying privacy issues including privacy law, compliance, and training.
 - i. Contracting Officers.
 - (1) Be aware of provisions to incorporate or make the appropriate modifications to contracts to include the attached CRD.
 - (2) After notification by the appropriate program official, incorporate the attached CRD into affected contracts via the laws, regulations, and DOE Directives clauses of the contracts.
8. ACRONYMS. See Appendix 1.
9. REFERENCES. See Appendix 2.
10. CONTACT. NNSA Privacy Act Officer, (505) 845-5680.

BY ORDER OF THE ADMINISTRATOR:



Lisa E. Gordon-Hagerty
Administrator

Appendixes

- 1. Acronyms
- 2. References

Attachments:

- 1. Contractor Requirements Document
- 2. NNSA Privacy Impact Assessments (PIAs) Procedures
- 3. System of Records Notice (SORNs) Procedures
- 4. Definitions

APPENDIX 1: ACRONYMS

- a. CIO – Chief Information Officer
- b. CFR – Code of Federal Regulations
- c. CPO – Chief Privacy Officer
- d. CRD – Contractor Requirements Document
- e. DOE – Department of Energy
- f. FOIA – Freedom of Information Act
- g. IARC – Information Assurance Response Center
- h. NA-GC – NNSA General Counsel
- i. NNSA – National Nuclear Security Administration
- j. OMB – Office of Management and Budget
- k. PAO – Privacy Act Officer
- l. PIA – Privacy Impact Assessment
- m. PII – Personally Identifiable Information
- n. SAOP – Senior Agency Official for Privacy
- o. SORN – System of Record Notice
- p. SD – Supplemental Directive
- q. U.S.C. – United States Code

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 2: REFERENCES

- a. 5 U.S.C. 552, *Freedom of Information Act* (FOIA)
- b. 44 U.S.C. 3541, et seq., *Federal Information Security Management Act* of 2014 (FISMA)
- c. 50 U.S.C. 2401 et seq., *National Nuclear Security Administration (NNSA) Act*
- d. Public Law 98-579, *Privacy Act* of 1974, as amended at 5 U.S.C. 552a
- e. Public Law 107-347, *E-Government Act* of 2002
- f. 2 Code of Federal Regulations (CFR) 200.79 – *Personally Identifiable Information (PII)*
- g. 10 CFR Part 1008, *Records Maintained on Individuals (Privacy Act)*
- h. 10 CFR Part 1004, *Freedom of Information Act (FOIA)*
- i. 36 CFR, Chapter 12, Subchapter B, *Records Management*
- j. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, dated 7-28-16
- k. OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, dated 12-23-16
- l. OMB Memorandum (M)-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, dated 10-30-15
- m. OMB M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, dated 7-1-16.
- n. OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, dated 9-15-16
- o. OMB M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, dated 11-4-16
- p. OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, dated 1-3-17
- q. Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information*, dated May 2012
- r. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, “Privacy Control Catalog.”

- s. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, dated April 2010
- t. DOE O 206.1, *Department of Energy Privacy Program*, dated 1-16-09
- u. DOE O 205.1B Chg 3 (PgChg), *Department of Energy Cyber Security Program*, dated 9-21-14
- v. SD 205.1, *Baseline Cybersecurity Program*, dated 7-6-17

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT **NNSA SD 206.1, *PRIVACY PROGRAM***

This Contractor Requirements Document (CRD) establishes the requirements for the National Nuclear Security Administration (NNSA) contractors with access to NNSA information systems. Contractors must comply with the requirements listed in this CRD.

Regardless of the performer of the work, site and facility management and support contractors are responsible for complying with and flowing down the appropriate requirements of this CRD to subcontractors at any tier, to the extent necessary, to ensure the contractors' compliance with the requirements of this CRD. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that are reasonable and would be incurred by a prudent person in the conduct of a competitive business.

1. REQUIREMENTS.

The contractor must:

- a. Ensure compliance with requirements of Office of Management and Budget (OMB) Circular A-130 Appendix II relevant to "Contractors and Third Parties."
- b. Ensure Privacy Impact Assessments (PIAs) are complete for federal information systems that process, contain, or store federal information under their management, and are provided to the site Privacy Representative and NNSA Privacy Act Officer (PAO) for review and signature. NNSA PIAs are to be completed on Form 206.1 <https://www.energy.gov/cio/downloads/oe-f-2061>. NNSA SD Form 206.1 must be completed and signed by the NNSA CPO for NNSA PIAs. A copy of the form can be found in Attachment 2.
- c. Assist with completing System of Records Notices (SORNs), where applicable.
- d. Ensure PII and *Privacy Act* information, in any format, electronic or hard copy, is protected and secured, and disposed of when no longer required in accordance to records disposition schedules.
- e. Establish processes to ensure all NNSA contractor employees receive training on privacy, including management of PII.
- f. Establish procedures that ensure the collection of social security numbers is only for the performance of the site's work, or to perform an agency function, and is authorized.
- g. Appoint a Privacy Representative.
- h. Manage NNSA incident and breach response capabilities involving PII in accordance with SD 205.1, *Baseline Cybersecurity*, and federal regulations, to include a process for tracking incidents and breaches.

- i. Report suspected or confirmed PII breaches as directed by SD 205.1, Attachment D, *Incident Management*. Based on mandated reporting requirements for PII, all suspected or confirmed incidents involving PII must be reported within 35 minutes to the Information Assurance Response Center (IARC) regardless of the type or system impact. This notification can be verbal or written via e-mail.

2. RESPONSIBILITIES.

Appointed Privacy Representative.

- a. Ensures that PII and *Privacy Act* information, as defined in DOE O 206.1, in any format, is protected and secured.
- b. Oversees local privacy development, implementation, and performance reporting activities.
- c. Ensures PIAs are completed for federal information systems that contain PII prior to the system receiving an authority to operate.
- d. Serves as liaison for local privacy activities, which includes, but is not limited to, privacy training for protection of PII and PIA completion.

ATTACHMENT 2 NNSA PRIVACY IMPACT ASSESSMENT (PIA) PROCEDURES

Note: This attachment applies to National Nuclear Security Administration (NNSA) contractors and federal employees.

This Attachment provides the procedures for completing NNSA Privacy Impact Assessment (PIA). The NNSA PIA process helps to ensure privacy protections are considered and implemented throughout the system life cycle.

When does a PIA need to be conducted?

Department of Energy (DOE) Order (O) 206.1, Appendix A, *Privacy Impact Assessments*, provides direction on when, why, and how to complete PIAs. The first step of the process is completing the first four questions of the PIA, which is the Privacy Needs Assessment (PNA) in DOE's template, <https://www.energy.gov/cio/downloads/privacy-impact-assessment-template-doe-form-2061>. The PNA will determine if a complete PIA is needed. PNAs must be completed for all NNSA Federal Information Systems.

PNAs/PIAs must be conducted when—

1. Designing, developing, or procuring information systems or information technology projects that collect, maintain, or disseminate information in identifiable form.
2. Modifying an information system, or every year.
 - PIAs should be updated whenever there is a change to the information system that affects privacy or creates new risks to privacy.

Within DOE/NNSA, the PNA is consolidated as part of the PIA.

Who Completes the PIA?

The PIA is the system owner's responsibility. The system owner, system developer, data owners, and the appointed Privacy Representative must work together to complete the PIA.

System owners must identify data that is collected and maintained in the information system as well as individuals who will access that data. The appointed Privacy Officer Representative must assess whether there are any threats to privacy. PIAs require collaboration with program experts as well as experts in the areas of information technology, cybersecurity, records management, and privacy.

Privacy Impact Assessment Document Review and Approval Process

1. The completed PIAs must be provided to the NNSA Privacy Act Officer (PAO) for review.

- The NNSA PAO provides the PIA to the NNSA Chief Privacy Officer (CPO) for approval and signature.

If the CPO indicates a corrective action is necessary for a PIA, the PIA is returned to the system owner. The system owner is responsible for identifying and implementing corrective actions prior to providing the PIA to the CPO.

The PIA flowchart in figure 1 illustrates this process.

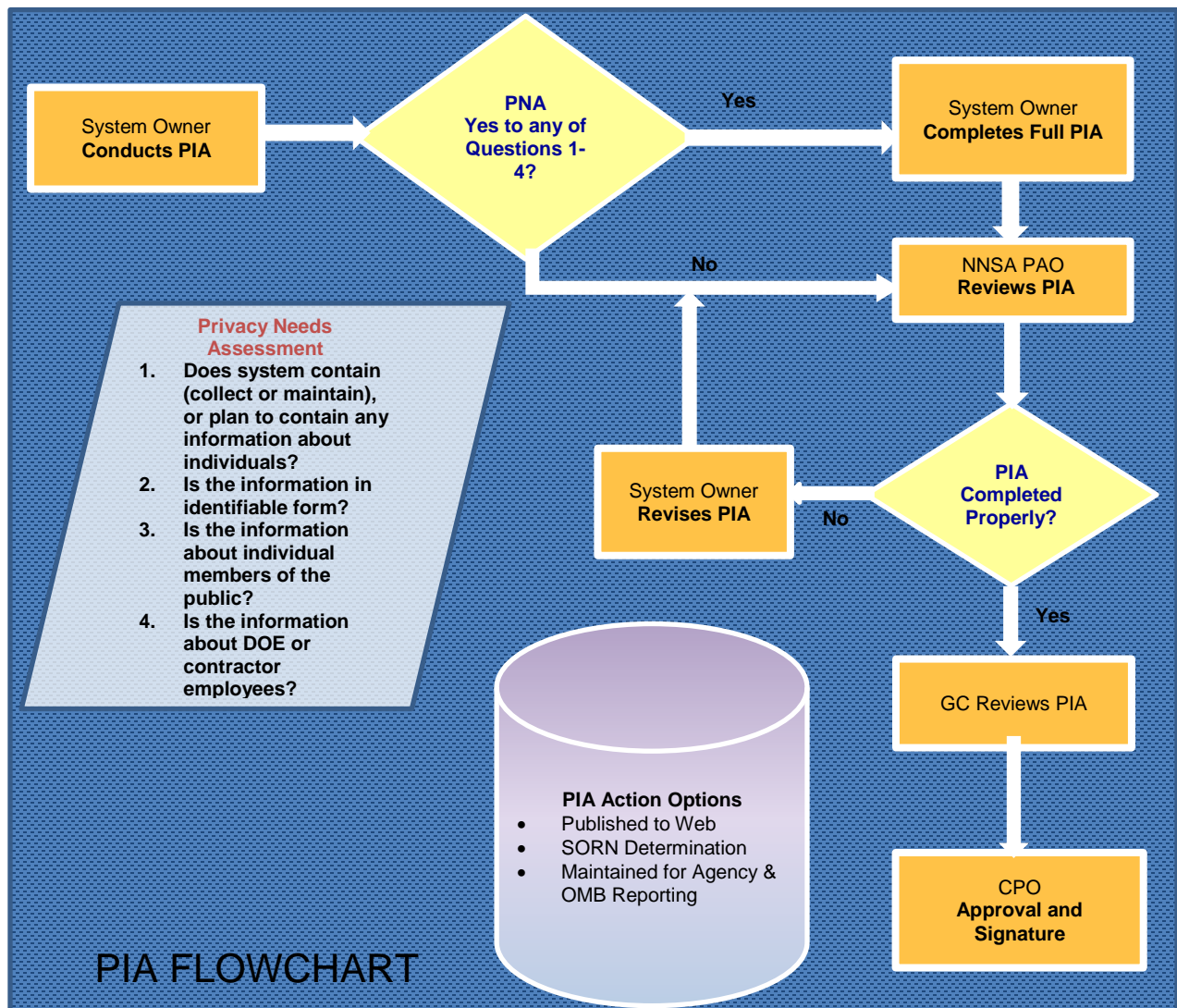


Figure 1. PIA Process

Below is the NNSA PIA signature page which must be completed for all NNSA PIAs.



The Office of the Associate Administrator
for Information Management and
Chief Information Officer

NNSA PRIVACY IMPACT ASSESSMENT SIGNATURE PAGE: ORG NAME – SYSTEM NAME

**Please complete form and return to the NNSA Privacy Act Officer Theresa.Follo@nnsa.doe.gov
No hand-written submissions will be accepted.**

SIGNATURE PAGE		
	Signature	Date
System Owner	_____ (Print Name) _____ (Signature)	_____ _____
Privacy Act Official (PAO) Concurrence	_____ (Print Name) _____ (Signature)	_____ _____
Cyber Security Approving Official (AO) Concurrence	_____ (Print Name) _____ (Signature)	_____ _____
NNSA General Counsel (GC)	_____ (Print Name) _____ (Signature)	_____ _____
For Contractor Sites Only Contracting Officer (CO) Representative (COR) Concurrence	_____ (Print Name) _____ (Signature)	_____ _____
Theresa Follo NNSA Privacy Act Officer (PAO)	_____ (Print Name) _____ (Signature)	_____ _____
Wayne Jones NNSA Deputy Associate Administrator for Information Management & Chief Information Officer/Chief Privacy Officer	_____ (Print Name) _____ (Signature)	_____ _____

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 3 SYSTEM OF RECORDS NOTICE (SORN) PROCEDURES

Note: This attachment applies to NNSA contractors and federal employees.

The *Privacy Act* requires agencies to publish a System of Records Notice (SORN) in the Federal Register and report to Congress when a new SORN is proposed or significant changes are made to a previously established system.

Criteria for Creating a New SORN

A new system of records is one for which no public notice is currently published in the Federal Register. A new SORN must be published when any one of the following criteria is met:

- A program, authorized by a new or existing statute or Executive Order (EO), maintains information on an individual and retrieves that information by personal identifier.
- There is a new organization of records resulting in the consolidation of two or more existing systems into one umbrella system, and the consolidation cannot be classified under a current SORN.
- It is discovered that records about individuals are being created and used, and that this activity is not covered by a currently published SORN. In this case, the Office of Management and Budget (OMB) requires the temporary suspension of data collection and disclosure.
- A new organization (configuration) of existing records about individuals that was not previously subject to the *Privacy Act* (i.e., was not a system of records) results in the creation of a system of records.

For assistance in creating a SORN, please contact the NNSA Privacy Act Officer.

Criteria for Amending a SORN

There are two types of amendments to SORNs: a significant alteration and a nonsignificant alteration.

If a significant alteration needs to be made to a system of records, the agency must immediately amend the SORN for that system of records and republish it in the Federal Register for a 30-day public comment period. Significant alterations also require the agency to send letters and a narrative to OMB and Congress explaining the alterations before the agency can begin to operate the system to collect and use the information. OMB and Congress require an additional 10 days to review the request, resulting in waiting period of 40 days before the agency can begin to operate the system.

Note: The proposed alterations to the existing system of records should be provided in the Supplementary Information in the introductory section of the notice, and the complete modified SORN should follow in its entirety.

Significant alterations include:

- Change in the number or type of individuals on whom records are maintained. (Changes that involve the number, rather than the type, of individuals about whom records are kept need to be reported only when the change alters the character and purpose of the system of records.)
- Expansion of the types or categories of information maintained. For example, if an employee file is expanded to include data on education and training, this is considered an expansion of the types or categories of information maintained.
- Change in the manner in which the records are organized, indexed, or retrieved that results in a change in the nature or scope of these records. Examples are splitting an existing system of records into two or more different system of records, which may occur in centralization or a decentralization of organizational responsibilities.
- Change in the purpose for which information in the system of records is used.
- Change in equipment configuration. This means changing the hardware or software on which the system of records operates to create the potential for either more or easier access.
- Change in procedures associated with the system in a manner that affects the exercise of an individual's rights.

For systems with nonsignificant alterations, such as a change in system owner, the only requirement is that a revised SORN be published in the Federal Register. The 30-day public comment period and 10-day OMB and Congress review period is not required for nonsignificant alterations.

Please consult the NNSA Privacy Act Officer for a final determination of the nature of any changes to a system of records.

How to Terminate an Existing System of Records

A system of records is considered to be terminated whenever the information is no longer accessed by individuals' names or other identifiers, or whenever it is consolidated with another system of records. Terminating a system may involve the physical destruction of records; it may involve purging the system of individual identifiers and maintaining the data in another form, such as statistical data; and it may involve altering the manner in which the records are accessed so that records are no longer accessed by the name of the subject individuals or other personal identifiers.

For assistance in terminating an existing system of records, please contact the NNSA Privacy Act Officer.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 4: DEFINITIONS

Note: This attachment applies to NNSA contractors and federal employees.

- a. **Breach:** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (A) a person other than an authorized user accesses, or potentially accesses, Personally Identifiable Information (PII) or (B) an authorized user accesses PII for a non-authorized purpose.
- b. **Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information; 44 U.S.C. 3502 – Definitions.
- c. **Information Technology:** (A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the 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 requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract. 40 U.S.C. 11101- Definitions
- d. **Incident:** An occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- e. **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or track an individual's identity, the term *PII* is necessarily broad. Assessments of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual should be performed. In performing the assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available—in any medium or from any source—that would make it possible to identify an individual. (OMB M-17-12).
- f. **Privacy Act Information:** Information that is required to be protected under the *Privacy Act* of 1974.

- g. Privacy Continuous Monitoring: A monitoring strategy that maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented.
- h. Privacy Impact Assessment (PIA): An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns.
- i. Record: Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.
- j. Senior Agency Official for Privacy (SAOP): The Deputy Assistant Secretary or equivalent level at an agency who leads and directs the agency's privacy program and carries out the privacy-related functions described in law and Office of Management and Budget (OMB) policies.
- k. System of Record: Any system on which PII or *Privacy Act* Information is stored that possesses an indexing or retrieval capability built into the system and from which records are retrieved about individuals by reference to a personal identifier.
- l. System of Record Notice (SORN): A group of any records 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 particular assigned to the individual.