SUPPLEMENTAL DIRECTIVE

NNSA SD 206.1A

Approved: 12-14-2023
Recertification Due: 12-14-2023

PRIVACY PROGRAM

National Nuclear Security Administration

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Information Management and Chief Information Officer

THIS PAGE INTENTIONALLY LEFT BLANK

PRIVACY PROGRAM

1. PURPOSE. This Supplemental Directive (SD) defines supplemental requirements and responsibilities to Department of Energy (DOE) Order (O) 206.1, *Department of Energy Privacy Program*, by establishing the roles of the Chief Privacy Officer (CPO) and the Privacy Act Officer (PAO) who will be responsible for implementing and managing an organizational privacy program.

2. AUTHORITY.

   a. DOE O 206.1, *Department of Energy Privacy Program*, current version.

   b. *Privacy Act of 1974 (Privacy Act)*, as amended, at Title 5 United States Code (U.S.C.) 552a.

   c. Section 208 of the *E-Government Act of 2002* (Public Law 107-347, 44 U.S.C. Ch 36).

3. CANCELLATIONS. National Nuclear Security Administration (NNSA) SD 206.1, *Privacy Program*, dated 6-22-2018.

4. 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 information and Personally Identifiable Information (PII) for NNSA.

   b. Contractors. Except for the equivalency in paragraph 4.c, Attachment 1, Contractor Requirements Document (CRD), and Attachments 2-6 set forth requirements that apply to site and facility management contracts. The CRD and the applicable Attachments must be included in management and operating (M&O) contracts and the subcontracts to the M&O contracts that manage, handle, control, maintain, access, and disseminate records, or manage federal information, and information systems that contain or store *Privacy Act* information or PII.

   c. Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order (EO) 12344, codified at 50 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.

5. SUMMARY OF CHANGES. The SD incorporates guidance from the National Institute of Standards and Technology (NIST) regarding its Privacy Framework; clarifies NNSA employee reporting responsibilities for *Privacy Act* violations and suspected or confirmed

PII breaches; establishes a PII breach reporting attachment in alignment with NNSA SD 205.1, *Baseline Cybersecurity Program*; clarifies Enterprise Authorizing Officials' (EAOs) responsibilities; and enables the Contracting Officer to delegate authority to sign Privacy Impact Assessments (PIAs).

6. BACKGROUND. This SD was developed using DOE O 206.1 as a baseline and is tailored to meet the mission requirements of NNSA. The SD provides guidance to ensure the appropriate management, oversight, and disposal of privacy information.

7. REQUIREMENTS. NNSA must:

   a. Establish and maintain a Privacy Program that complies with all applicable federal laws, regulations, and guidance to include, at a minimum, EOs, Office of Management and Budget (OMB) Memoranda, Committee on National Security Systems (CNSS) Instructions and Directives, and policies referenced in Attachment 6.

   b. Require compliance with the *Privacy Act* and PIA guidance. NNSA PIAs must be completed on the current NNSA SD Form 206.1 and be signed by the NNSA CPO.

   c. Implement the requirements and safeguards identified in DOE O 206.1.

   d. Establish an Enterprise Privacy Framework that follows the NIST Privacy Framework.

   e. Define the roles and responsibilities required to implement the NNSA Privacy Program requirements in accordance with DOE O 206.1.

   f. Appoint a CPO with NNSA-wide accountability for information privacy issues.

   g. Appoint a PAO responsible for managing the NNSA Privacy Program, per DOE O 206.1.

   h. Appoint a Privacy Representative (PR) to provide oversight at their respective program or site.

   i. Establish processes to ensure all NNSA employees complete privacy training that includes the management of PII.

   j. Collect Social Security numbers (SSNs) only for the performance of the program or office's work and retain them as needed in order to perform work or an agency function and as authorized or as required by law. Disposition or retention of documents or inventory containing SSNs must be in accordance with the current versions of DOE O 206.1 and DOE O 243.1, *Records Management Program*.

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 with records disposition schedules. In the event of a *Privacy Act* violation or PII breach, appropriate management officials must be notified in accordance with the incident reporting process outlined in Attachment 4, Reporting Privacy Act Violations and Breaches of Personally Identifiable Information.

8. RESPONSIBILITIES.

a. Associate Administrator for Information Management and Chief Information Officer (NA-IM).

Serves as the NNSA CPO. The NNSA CPO responsibilities may be delegated as needed.

b. NNSA Chief Privacy Officer.

(1) Oversees, coordinates, and facilitates the NNSA Privacy Program by ensuring the program is in full compliance with federal laws, regulations, and policies related to the maintenance, collection, dissemination, and use of privacy information.

(2) Coordinates with the DOE Senior Agency Official for Privacy (SAOP) on Department-level privacy concerns and issues.

(3) Participates as a member in DOE's and NNSA's Privacy Incident Response Team, as appropriate.

(4) Approves PIAs and System of Records Notices (SORNs) for NNSA.

(5) Appoints the NNSA PAO, who is responsible for implementing the *Privacy Act* activities in accordance with the *E-Government Act of 2002* and OMB Memorandum (M)-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

(6) Approves all NNSA privacy policies and guidance.

c. NNSA Privacy Act Officer.

(1) Manages the NNSA Privacy Program.

(2) Coordinates with and supports the DOE SAOP on NNSA privacy activities to include PIA and SORN management, privacy training, annual incident response plan reviews, reporting of privacy breaches, and managing PII incident management guidance.

(4) Coordinates with Information Assurance Response Center (IARC) on notification of reported privacy breaches and PII-related incidents.

(5) Develops privacy policy and training guidance for the proper handling, transmitting, and storing of privacy information and the preparation of PIAs and ensures employees and contractors receive training.

(6) Coordinates with and advises appointed PRs on the inclusion of privacy, confidentiality, and data security requirements in site-level policies and programs.

(7) Ensures PIAs are up to date and complete for all unclassified information systems that maintain information.

(8) Conducts site reviews of privacy practices regarding collection or disclosure of personal information in privacy systems of records.

(9) Provides mandatory reports on the status of NNSA privacy protections to DOE and OMB.

(10) Advises and provides guidance to both NNSA Element and Contractor PRs about conducting, writing, and completing the NNSA PIA and SORN process and privacy management.

(11) Ensures privacy program requirements are integrated throughout NNSA programs.

(12) Establishes agency level procedures to ensure the collection of SSNs is only for the performance of work or an agency function and is authorized.

d. Program/Functional/Field Office Manager. Appoints and oversees their NNSA Element PR.

e. NNSA Element PR.

(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) Coordinates with the NNSA PAO, NNSA General Counsel (NA-GC) and Field Counsel in providing legal review and interpreting and applying privacy laws, compliance, and training.

(4) Establishes internal procedures to ensure the collection of SSNs is only for the performance of work or an agency function and is authorized. Ensures

that the disposition or retention of documents or inventory containing SSNs complies with DOE O 243.1C.

(5) Serves as the liaison for local privacy activities, including the completion of PIAs.

f. Enterprise Authorizing Official. Reviews and approves PIAs.

g. Authorizing Official (AO) and Authorizing Official Designated Representative (AODR).

Supports NNSA Element PR oversight of privacy activities under their cognizance, including the use of PIAs and associated impact to the overall cybersecurity posture.

h. NNSA Employees.

(1) Ensures PII and privacy information is securely handled with the appropriate safeguards in accordance with established DOE procedures.

(2) Completes annual privacy training provided by DOE.

(3) Reports all *Privacy Act* violations and suspected or confirmed PII breaches, in accordance with Attachment 4.

(4) Cooperates with incident response teams that are investigating or attempting to resolve incidents involving PII.

i. System Owners.

(1) Manage and monitor information systems under their purview to ensure compliance in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource*, other applicable federal guidance, and DOE O 206.1.

(2) Drafts the site PIAs for conformance to requirements of DOE O 206.1, this SD, and SD 205.1, in coordination with the NNSA Element PR.

(3) Determines, with the PAO and CPO, the appropriate allocation of resources dedicated to the protection of PII systems.

j. NNSA General Counsel (NA-GC).

(1) Serves as a subject matter expert regarding *Privacy Act* and *Freedom of Information Act* matters to ensure that NNSA provides a complete, legal, and prompt response to all individual requests for *Privacy Act*-protected

information, where appropriate. Manages *Privacy Act* requests to dispense timely information to requesting parties.

(2) Provides legal review and concurrence before publishing any Departmental SORN in the Federal Register.

(3) Reviews and concurs with PIAs in accordance with Attachment 2.

(4) Provides legal expertise to all NNSA Elements in interpreting and applying privacy issues, including privacy law, compliance, and training.

k. Contracting Officers.

(1) Incorporate or make the appropriate modifications to contracts to include the attached CRD after notification by the appropriate program official.

(2) Sign PIAs in accordance with Attachment 2. The Contracting Officer may delegate this authority to the Contracting Officer Representative.

9. REFERENCES. See Attachment 6.

10. CONTACT. NNSA Privacy Act Officer at nnsana-imprivacyprogram@nnsa.doe.gov.

BY ORDER OF THE ADMINISTRATOR:

Jill Hruby
Administrator

Attachments:

1. Contractor Requirements Document
2. NNSA Privacy Impact Assessments (PIAs) Procedures
3. System of Records Notice (SORN) Procedures
4. Reporting *Privacy Act* Violations and Breaches of Personally Identifiable Information (PII)
5. Definitions
6. References

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

This Contractor Requirements Document (CRD) establishes the requirements for the National Nuclear Security Administration (NNSA) contractors who manage, operate, and access NNSA and Department of Energy (DOE) information systems. Contractors must comply with the requirements listed in this CRD and all applicable Attachments. Regardless of the performer of the work, contractors are responsible for complying with and incorporating the appropriate CRD requirements into subcontractor contracts at any tier, to the extent necessary, to ensure the contractors comply with the requirements. The contractors must ensure that they and their subcontractors incur only those costs that are reasonable and that would be incurred by a prudent person in the conduct of a competitive business. Contractors and subcontractors are responsible for complying with any attachment referenced in and made a part of this CRD.

1. REQUIREMENTS. The contractor must:

   a. Ensure compliance with privacy requirements regarding Executive Orders and Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource,* Appendix II., 5.d., "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 Representatives (PRs), system Authorizing Official (AO) and Authorizing Official Designated Representative (AODR), and NNSA Privacy Act Officer (PAO) for review.

      (1) NNSA PIAs must be completed using the most current version of the PIA Template, which must be signed and approved by the NNSA Chief Privacy Officer (CPO).

      (2) The current version of the PIA Template is available from the Office of the Associate Administrator for Information Management and Chief Information Officer, NNSA PAO, at nnsana-imprivacyprogram@nnsa.doe.gov.

   c. Assist with completing System of Records Notices (SORNs).

   d. Ensure Personally Identifiable Information (PII) and information subject to the *Privacy Act of 1974 (Privacy Act)*, as amended, in any format, is protected, secured, and disposed of when no longer required, in accordance with records disposition schedules.

   e. Establish processes to ensure all NNSA contractor employees receive training on privacy, including management and protection of PII.

f. Establish procedures that ensure the collection of Social Security Numbers (SSNs) is only for the performance of the site's work or to perform an agency function and is authorized.

g. Appoint a PR.

h. Manage NNSA incident and breach response capabilities involving PII in accordance with Supplemental Directive (SD) 205.1, *Baseline Cybersecurity Program*, and federal regulations, to include a process for tracking incidents and breaches.

i. Report suspected or confirmed PII breaches SD 205.1. Based on mandated reporting requirements for PII, all suspected or confirmed incidents involving PII must be reported within 60 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.

j. Dispose or retain documents or inventory containing SSNs in accordance with DOE Order (O) 206.1, *Department of Energy Privacy Program*, and DOE O 243.1, *Records Management Program*.

2. RESPONSIBILITIES.

a. Site Chief Information Officer or Equivalent.

Coordinates with the NNSA PAO on privacy concerns and issues, including ensuring timely responses and reporting of privacy breaches and initiating investigations and corrective actions.

b. Site Privacy Representative (PR).

(1) Serves as privacy liaison and oversees local privacy development, implementation, privacy training, and performance reporting activities at their respective program office or site.

(2) Participates in enterprise-wide privacy efforts.

(3) Coordinates with the system owner to ensure PIAs are completed for federal information systems that contain PII prior to the system receiving an authority to operate.

(4) Coordinates with NNSA General Counsel (NA-GC) and Field Counsel in providing legal review and interpreting and applying privacy issues, including privacy law, compliance, and training.

(5) Manages SSN collection and use for their site, in accordance with Requirement f. above.

c. System Owner.

(1) Oversees, manages, and monitors information systems under their purview to ensure compliance in accordance with OMB Circular A-130 and other applicable federal guidance and laws, including DOE O 206.1 on the safeguarding of privacy information.

(2) Determines whether any change to the information stored in their system requires initiation of a PIA, in accordance with Attachment 2, and that the use of PII conforms to the applicable SORN published in the Federal Register.

(3) In coordination with the PR(s), reviews the PIAs for conformance to requirements of DOE O 206.1, this SD, and SD 205.1.

(4) Determines, with the NNSA PAO, the appropriate allocation of resources dedicated to the protection of PII systems.

d. Cybersecurity Approving Official (Authorizing Official, Information System Security Manager (ISSM)/Information System Security Officer (ISSO).

Reviews and concurs with approval of PIAs in accordance with Attachment 2.

e. Authorizing Official Designated Representative (AODR).

Reviews and signs, as appropriate, PIAs in accordance with Attachment 2.

f. Field Counsel.

Reviews and concurs with approval of PIAs in accordance with Attachment 2.

ATTACHMENT 2: NNSA PRIVACY IMPACT ASSESSMENT PROCEDURES

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in Attachment 1, Contractor Requirements Document (CRD), contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that incorporate the CRD.

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

When does a PIA need to be conducted?

Department of Energy (DOE) Order (O) 206.1A, *Department of Energy Privacy Program,* Attachment 2, *DOE Privacy Impact Assessments Procedures*, provides direction on the completion of PIAs. The first step of the process, Privacy Threshold Assessment (PTA), determines if a PIA is necessary for a system. PTAs must be completed for all NNSA federal information systems. The NNSA PTA template is available by emailing the NNSA privacy mailbox at nnsana-imprivacyprogram@nnsa.doe.gov. PTAs/PIAs must be completed every three years, or when:

1. Designing, developing, procuring, or operating information systems or information technology projects that collect, maintain, or disseminate information in identifiable form.

2. Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons.

3. Updates are made to an information system that impact the way information is handled that may pose additional privacy risks.

Within DOE/NNSA, the PTA is consolidated as the first 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 (PR) must work together to complete the PIA. System owners must identify data that is collected and maintained in the information system as well as identifying individuals who will access that data. The PR must assess whether there are any threats to privacy. PIAs require collaboration with program 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. All PIAs must be submitted according to the latest version of the NNSA PIA

template and the PIA information entered into NNSA Archer or other Enterprise Governance, Risk, and Compliance tool as designated by the PAO. The NNSA PIA template is available from the PAO or by emailing nnsana-imprivacyprogram@nnsa.doe.gov.

2. The NNSA PAO provides the PIA to the NNSA Chief Privacy Officer (CPO), or delegate, for approval and signature.

If the CPO or Authorizing Official/Authorizing Official Designated Representative 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.

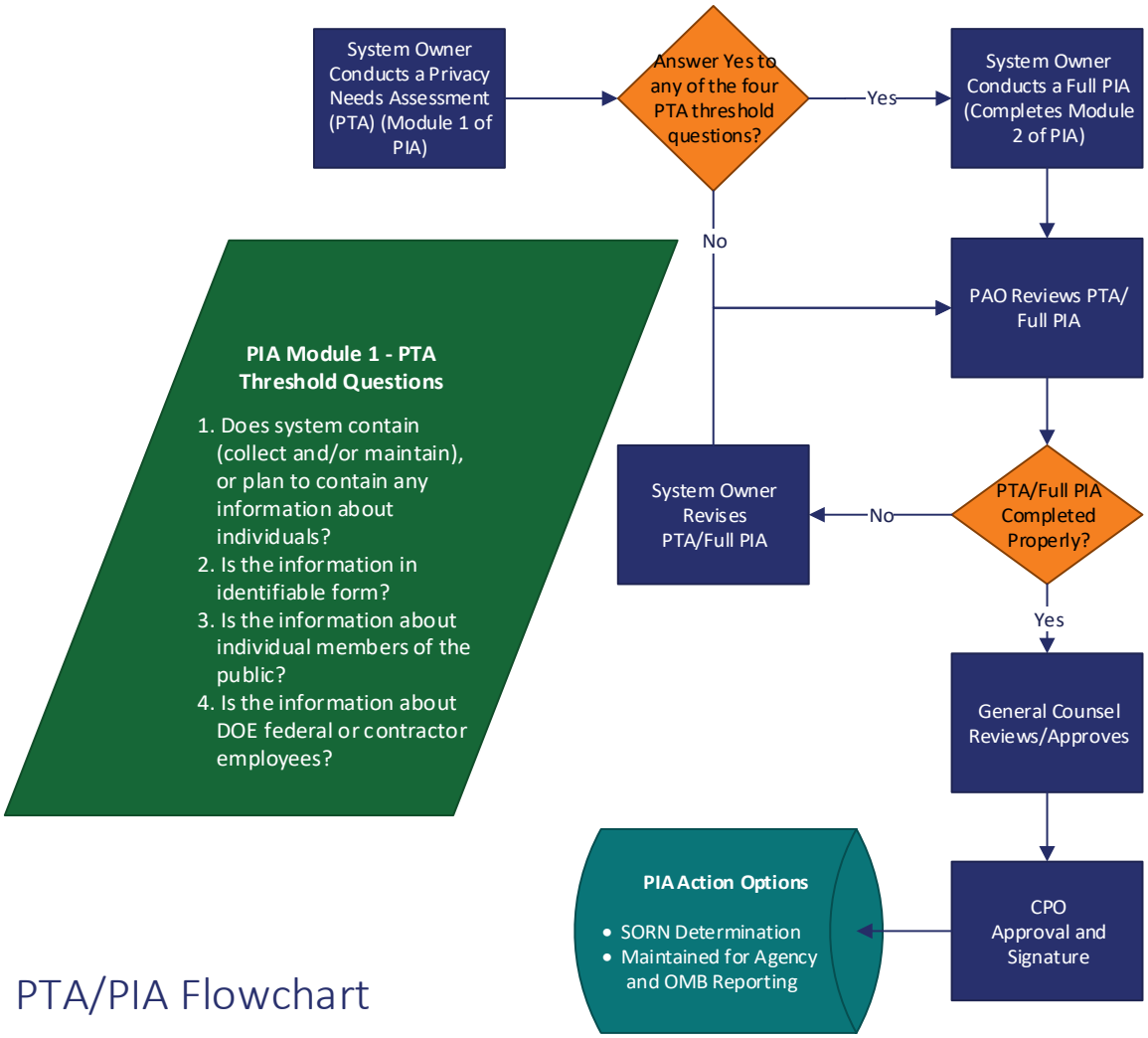

Figure 1. PIA Process

ATTACHMENT 3: SYSTEM OF RECORDS NOTICE (SORN) PROCEDURES

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in Attachment 1, Contractor Requirements Document (CRD), contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that incorporate the CRD.

The *Privacy Act of 1974 (Privacy Act)*, as amended, requires agencies to publish a 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 SORN 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, 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 (SOR)) results in the creation of a SOR.

For assistance in creating a SORN, please contact the NNSA Privacy Act Officer (PAO) at nnsana-imprivacyprogram@nnsa.doe.gov.

Criteria for Amending a SORN

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

If a significant alteration needs to be made to a SOR, the agency must immediately amend the SORN for that SOR and re-publish 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 a waiting period of 40 days before the agency can begin to operate the system.

Note: The proposed alterations to the existing SOR should be provided as 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 SOR.

- 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 how records are organized, indexed, or retrieved, which results in a change in the nature or scope of these records. For example, splitting an existing SOR into two or more different systems of records, which may occur in centralization or decentralization of organizational responsibilities.

- Change in the purpose for which information in the SOR is used.

- Change in equipment configuration.

- Change in procedures associated with the system in a manner that affects the exercise of an individual's rights.

For systems with non-significant 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 Congressional review period are not required for non-significant alterations.

Please consult the NNSA PAO for a final determination regarding any changes to a SOR.

How to Terminate an Existing SOR

A SOR is terminated whenever the information is no longer accessible by individuals' names or other identifiers, or whenever it is consolidated with another SOR. Terminating a system may involve the physical destruction of records or purging the system of individual identifiers and maintaining the data in another form, such as statistical data, in which the records are no longer accessible by the name of the individuals or other personal identifiers.

For assistance in terminating an existing SOR, please contact the NNSA PAO at nnsana-imprivacyprogram@nnsa.doe.gov.

ATTACHMENT 4: REPORTING PRIVACY ACT VIOLATIONS AND BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in Attachment 1, Contractor Requirements Document (CRD), contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that incorporate the CRD.

This attachment provides additional guidance regarding the information required for reporting *Privacy Act of 1974*, as amended, violations and Personally Identifiable Information (PII) breaches. In addition to the information required by NNSA Supplemental Directive 205.1, *Baseline Cybersecurity Program*, the incident report must include:

- Date and time of discovery of the breach;
- Description of the circumstances surrounding the breach;
- Type(s) of PII involved;
- Number of affected individuals;
- Whether the affected individuals are members of the public;
- The location of the PII (physical or in an Information Technology system);
- Whether the PII was secured or encrypted; and
- A point of contact familiar with the breach who will be able to answer questions and provide updates until the report is officially closed.

Incidents, either electronic or paper-based, must be reported within one hour to the Information Assurance Response Center (IARC) and the NNSA Privacy Act Officer (PAO), regardless of type or system impact. This notification must be submitted via email to iarc@iarc.nv.gov and nnsana-imprivacyprogram@nnsa.doe.gov. Classified reports must be submitted to iarc@iarc.doe.sgov.gov (NSN) or iarc@iarc.gov (ESN).

ATTACHMENT 5: DEFINITIONS

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in Attachment 1, Contractor Requirements Document (CRD), contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that incorporate the CRD.

a. Breach: See Department of Energy (DOE) Order 206.1, *Department of Energy Privacy Program*.

b. 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.

c. 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. In performing an 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. More information on how to prepare for and respond to a breach of PII can be found in the Office of Management and Budget Memorandum 17-12.

d. Privacy Act Information: Required to be protected under the *Privacy Act of 1974 (Privacy Act)*, as amended.

e. Privacy Impact Assessment (PIA): An analysis of how privacy information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements; 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.

f. Privacy Threshold Assessment (PTA): The first step in the PIA process, previously known at DOE as a Privacy Needs Analysis. PTAs are structured to assess the collection and intended use of PII. PTAs use threshold questions to determine whether a full PIA is necessary.

g. System of Records (SOR): Any system in 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.

h. System of Records 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. Agencies are required to publish new or revised notices in the Federal Register regarding the existence or character of the system.

ATTACHMENT 6: REFERENCES

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in Attachment 1, Contractor Requirements Document (CRD), contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that incorporate the CRD.

a. 5 United States Code (U.S.C.) § 552, *Freedom of Information Act*.

b. 44 U.S.C. § 3541 et seq., *Federal Information Security Management Act of 2014*.

c. 50 U.S.C. § 2401 et seq., *National Nuclear Security Administration (NNSA) Act.*

d. Public Law (Pub. L.) 98-579, *Privacy Act of 1974*, as amended, at 5 U.S.C. § 552a.

e. Pub. L. 107-347, *E-Government Act of 2002.*

f. Title 2, Code of Federal Regulations (CFR) 200.79, *Personally Identifiable Information (PII).*

g. Title 10 CFR 1008, *Records Maintained on Individuals (Privacy Act).*

h. Title 10 CFR 1004, *Freedom of Information Act (FOIA).*

i. Title 36 CFR, Chapter 12, Subchapter B, *Records Management.*

j. Volume 74 Federal Register 994, *Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records*, dated 1-9-2009.

k. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*.

l. OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

m. OMB Memorandum (M)-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

n. OMB M-05-08, *Designation of Senior Agency Officials for Privacy*.

o. OMB M-06-15, *Safeguarding Personally Identifiable Information*.

p. OMB M-06-19**,** *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*.

q. OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*.

r. OMB M-16-14, Category Management Policy 16-2: *Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*.

s. OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.

t. OMB M-17-06, *Policies for Federal Agency Public Websites and Digital Services*.

u. OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

v. Department of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information*.

w. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

x. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

y. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.

z. DOE Order (O) 206.1, *Department of Energy Privacy Program*, current version.

aa. DOE O 205.1, *Department of Energy Cyber Security Program*, current version.

bb. Supplemental Directive 205.1, *Baseline Cybersecurity Program*, current version.