U.S. Department of Energy
Washington, DC

ORDER

DOE O 206.1A

Approved: 1-19-2024

SUBJECT: DEPARTMENT OF ENERGY PRIVACY PROGRAM

1. PURPOSE.

   a. Enable accomplishment of the Department's mission and fulfill Federal privacy requirements while allowing Departmental Elements (DEs) programmatic and operational flexibility, enhancing privacy risk management, enabling effective protection of personally identifiable information (PII), supporting implementation and operations involving PII, addressing roles and responsibilities, and setting standards for performance across all levels of the Department.

   b. Provide Departmental oversight to ensure compliance with Federal statutes, regulations and Departmental Directives related to privacy.

2. CANCELS/SUPERSEDES. DOE O 206.1 Chg 1 (MinChg), Department of Energy Privacy Program, dated 11-01-2018, is canceled. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Contractor requirement documents (CRDs) that have been incorporated into or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Applicability. This Order applies to all Departmental Elements, including those created after the Order is issued.

      The Administrator of the National Nuclear Security Administration (NNSA) must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

      Note: The NNSA issues a Supplemental Directive to provide additional requirements and amplifying guidance on implementation of the requirements of Federal law, executive order, regulation, policy, and DOE O 206.1A for its component activities.

b. The Head of the DOE Office of Intelligence and Counterintelligence (DOE-IN) may provide additional requirements and guidance on the implementation of O 206.1A for national security systems and other privacy matters under the purview of their office.

c. DOE Contractors. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Order that will apply to contracts that include the CRD or its requirements. The CRD will apply to the extent set forth in each contract.

d. Equivalencies/Exemptions for DOE O 206.1A. Equivalencies and exemptions to this Order are processed in accordance with DOE O 251.1, Departmental Directives Program, current version.

e. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 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 Order for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS.

a. To implement the DOE Privacy Program, the Department maintains:

(1) An Enterprise Privacy Program (EPP), which is the responsibility of the DOE Chief Privacy Officer (CPO) to manage, in consultation with the Senior Agency Official for Privacy (SAOP) and in coordination with the Director of Privacy Compliance and Management. The EPP operates the Department's compliance with Federal privacy laws and establishes Department-level privacy controls and manages the Department's external reporting responsibilities. This program is also referenced as "DOE HQ Privacy" in various sections and appendices of this Directive.

(2) A Privacy Incident Response Plan, which defines a process for incident reporting that requires all suspected and confirmed incidents and breaches involving PII in any format, or information systems containing PII, under DOE or DOE contractor control must be identified, mitigated, categorized, and reported to Integrated Joint Cybersecurity Coordination Center (iJC3) or Information Assurance Response Center (IARC) in accordance with DOE O 205.1C and the Department's Privacy Incident Response Plan procedures and guidance.

(3) A Privacy Continuous Monitoring (PCM) program, responsible for maintaining ongoing situational awareness of threats and vulnerabilities that may pose privacy risks. The PCM establishes the Department's processes for the implementation of privacy controls as defined by guidance issued by the National Institutes of Standards and Technology (NIST). The PCM conducts ongoing privacy control assessments to verify the effectiveness of privacy controls selected for implementation; provides tools and processes for assessing compliance with applicable statutory, regulatory, and policy requirements, and provides tailored training to employees and contractors with assigned privacy compliance roles and responsibilities.

(4) In support of the preceding paragraphs 4.a.(1), (2), and (3), the SAOP is authorized to issue non-binding amplifying guidance on privacy, which may be adopted or tailored to individual DE/Site needs to meet requirements. This authority can be delegated to the CPO of DOE and NNSA as appropriate.

b. The following privacy requirements apply to all Departmental Elements:

(1) Safeguarding PII.

(a) Ensure compliance with privacy requirements, specifically those included in the References section below.

(b) PII, regardless of whether it is in paper, verbal, or electronic form, must be protected from unauthorized access or disclosure throughout its lifecycle.

(c) DEs shall limit the collection, use, retention, sharing, and dissemination of PII to only that information which is specifically needed to carry out official business of the Department or a distinct mission requirement.

(d) DEs shall eliminate the collection and use of Social Security Numbers (SSNs) except when justification for use is required to implement a statute or regulation. DEs shall develop plans to eliminate unauthorized and unnecessary SSN collection and use in DOE information systems and programs, whether in electronic or paper form. DEs are encouraged to evaluate and transition to the use of alternative identifiers (such as the OneID solution).

(e) DEs shall ensure that employees receive annual training on the identifying, safeguarding, handling, and protection of PII.

(f) In the event of a breach or an incident, DEs will follow reporting requirements as identified in either DOE O 205.1, current version, or NNSA SD 205.1, current version. For incidents or breaches involving PII, either suspected or confirmed, the following additional steps must be taken:

1 Data breaches or incidents involving PII in printed, verbal, or electronic form must be immediately reported.

2 In addition to following above stated reporting requirements, the incident or breach should be reported to the Local Privacy Officer (LPO) for their awareness.

(2) The Privacy Act.

(a) DEs shall support Departmental compliance with the Privacy Act. The Privacy Act governs a Federal agency's ability to collect, use, maintain, or disseminate a record about an individual. The Privacy Act also grants individuals increased rights of access and amendment of agency records maintained on themselves and restricts disclosure of records.

(b) Information collected under the Privacy Act must be stored in a Privacy Act System of Records (SOR) with public notice, known as a System of Records Notice (SORN), published in the Federal Register. See Appendix B for guidance on Privacy Act requirements for creating new or modifying existing Departmental SORNs.

(c) Non-compliance with the Privacy Act carries criminal and civil penalties.

(3) Privacy Compliance Requirements.

(a) The Department must provide annual training and awareness for DOE Federal and contractor employees to ensure personnel are cognizant of their responsibilities for:

1 Identifying and safeguarding PII;

2 Complying with the Privacy Act;

3 Recognizing the different safeguard obligations created by privacy laws and relevant authorities; and

4 Reporting suspected and confirmed breaches of PII immediately.

(b) Privacy Threshold Assessments and Privacy Impact Assessments.

1 DEs shall ensure that all information systems containing PII have a Privacy Threshold Assessment (PTA) and/or a Privacy Impact Assessment (PIA) approved by the CPO or designated official. PIAs must be reviewed and updated in accordance with Attachment 2.

(c) Privacy Act System of Record Notices (SORNs).

1 DEs will ensure that PII subject to the Privacy Act is maintained under an appropriate SORN.

(d) The Department shall maintain an inventory of systems that collect, use, maintain, and share PII, and an inventory of all information holdings that use or maintain Social Security Numbers (SSNs). DEs will assist in maintaining this inventory.

5. RESPONSIBILITIES.

a. Secretary of Energy (S1).

(1) Designates the Department's SAOP.

(2) Designates the standing group of Departmental representatives to the Privacy Incident Response Team (PIRT). The positions participating in the PIRT are summarized in Appendix A.

(3) Reports breaches that the PIRT determines to be Major Incidents to the appropriate Congressional Committees and to the White House no later than seven (7) days after the date on which there is a reasonable basis to conclude that a breach that constitutes a Major Incident has occurred.

(4) For matters involving privacy incident response for Major Incidents, responsibilities include:

(a) Deciding whether the Department will provide notification to affected individuals.

(b) Determining whether additional identity protection services will be provided to individuals affected by a breach involving PII.

(c) Determining which Department Staff Office or DE is responsible for covering the financial costs of notification and corrective services, if needed. Generally, this will be the Staff Office or DE responsible for the breach.

b. Deputy Secretary of Energy (S2).

(1) Serves as the Secretary's designee in executing the Secretary's privacy incident response responsibilities under this plan, either for specific breaches or when the Secretary is unavailable.

(2) Determines if and what further actions are necessary in the event of non-concurrence between the SAOP and the CIO, or between the SAOP and the PIRT, where the PIRT is convened.

c. Secretarial Officers/Heads of Departmental Elements.

(1) Maintain overall responsibility and accountability for ensuring the DEs' implementation of privacy protections and management of privacy risk in accordance with Federal laws, regulations, Departmental policies, and Directives.

(2) Ensure the appointment of site Local Privacy Officers (LPOs) for their Departmental Elements, including Local Privacy Act Officers (LPAO) and Privacy Points of Contact (PPOC), and consider appointing an individual to each role for full coverage of all privacy activities.

(3) Use a risk-based and tailored approach to flow down the requirements and responsibilities of this Order to all subordinate organizational levels through assigned local privacy officers.

(4) Consult, inform, and coordinate with the DOE SAOP to resolve cross-DE issues regarding privacy risk.

(5) Identify systems that process PII and ensure systems are managed to:

(a) Limit access to only those individuals whose work requires access to the PII.

(b) Ensure programs minimize the collection of PII to only that which is legally authorized or required to conduct business operations necessary for the proper performance of a documented DOE function.

(c) Implement appropriate security and privacy controls and continuous monitoring of controls to protect PII throughout its lifecycle.

(6) Designate representatives to participate on the PIRT, if convened, at the request of the SAOP. Provide additional representatives to support the CPO in assessing, investigating, and implementing corrective action for breaches involving PII that have significant impacts on the Department, DE, Program Office/Site, or DOE IT systems or networks.

(7) Submit any optionally developed DE- or Site-specific breach response plan annually to the SAOP for review and approval. Appendix A allows DEs and Sites to develop optional DE-specific or Site-specific breach response plans provided they reflect the processes and requirements of the Department's breach response plan in Appendix A, OMB Memorandum 17-12, and other applicable law, and are approved annually by the SAOP.

(8) Ensure that all DEs/Sites maintain a process for tracking incidents involving breaches of PII. At a minimum, this tracking mechanism should include the dates and times of events, whether the breach involved physical files or electronic information, and decisions and corrective actions. Each DE/Site will provide tracking reports to the SAOP on request.

(9) Ensure responsibility for all costs associated with remediation including notification of affected or potentially affected individuals for breaches originating within their Element.

(10) Ensure subordinate organizations engage and coordinate with the Department's PCM program regarding the selection, implementation, and assessment of privacy controls outlined in NIST Special Publication 800-53, current version.

d. Heads of Program Offices/Heads of Field Offices/Heads of Site Offices.

(1) Ensure personnel receive training on privacy matters.

(2) Ensure the completion of PIAs for Systems[1] with PII in accordance with the requirements of this Order and all Appendices and Attachments as required by law.

(3) Ensure privacy notices are posted for IT Systems, applications, and PII collection points in accordance with Federal law, regulations, and OMB directives.

(4) Implement their DE's plans to eliminate the unnecessary collection and use of SSNs.

(5) Ensure that Program or Site Offices' privacy compliance documentation, including PIAs, are up-to-date and available to serve as a resource for incident response or breach investigations.

[1] System refers to Federal Information Systems and Contractor Information Systems, as defined in Attachment 3 of this Order.

(6) Support the SAOP and the CPO in conducting annual reviews of the Program or Site Offices' privacy incident response plans and periodic audits of Program or Site Offices' breach response activities, if applicable.

(7) The SAOP has the discretion to further delegate specific privacy authorities, dependent on circumstances and program maturity.

e. Head of the Office of Intelligence and Counterintelligence (DOE-IN).

(1) Appoints a Civil Liberties and Privacy Officer to implement the requirements of Federal law, executive order, regulation, policy and DOE O 206.1A for national security matters under the purview of DOE-IN.

(2) Provides additional requirements and guidance on the implementation of O 206.1A for national security systems and other privacy matters under the purview of their office.

(3) Coordinates with the SAOP and CPO on DOE-IN's privacy program and guidance.

f. Senior Agency Official for Privacy (SAOP).

(1) Oversees, coordinates, and facilitates the Department's compliance with authorities governing privacy protection.

(2) Issues Departmental privacy policy.

(3) Ensures the protection of PII both at rest and in transit within, across, and external to DOE IT systems and networks, as required.

(4) Serves as the Secretary's authorized designee for the operational management of privacy incident response. The SAOP may also be designated additional incident response responsibilities, except for decisions related to the Department's response to a Major Incident.

(5) Determines whether a breach meets the criteria of a Major Incident, in collaboration with members of the PIRT.

(6) Determines whether a breach of PII reported by a DE, Program Office, or Site should be handled by Headquarters staff, based on:

(a) The scope and impact of the breach, including the number of affected persons;

(b) Whether the breach involves at least two or more DOE Elements or Offices; or

(c) The SAOP's determination that it is otherwise significant.

(7) Convenes and chairs the PIRT. The PIRT shall always be convened when a breach constitutes a Major Incident.

(8) Develops and conducts tabletop exercises for PIRT members at least annually and provides additional training as appropriate.

(9) Advises the Secretary on whether and when to notify individuals affected or potentially affected by a breach and makes recommendations regarding potential services to provide to affected individuals, to include credit monitoring or identity restoration services.

(10) Reviews and approves DE-specific breach response plans submitted by Secretarial Officers/Heads of DEs/Heads of Program Offices/Heads of Field Elements.

(11) Conducts annual reviews of DE-specific breach response plans and periodic audits of DE breach response activities, if applicable.

(12) Coordinates with appropriate agency officials to ensure that law enforcement and the Office of Inspector General (OIG) are notified in the event of a breach involving alleged or suspected criminal activity.

(13) Reports metrics on breaches involving PII impacting the Department under quarterly and annual Federal Information Security Modernization Act (FISMA) reporting requirements.

(14) Issues Departmental guidance to DEs/Sites to lessen the risk of privacy breaches (e.g., reducing the use of SSNs in DOE information systems and collections, and encouraging the use of encryption, password-protection, or an appropriate secure transmission option when sending PII through electronic means).

(15) Maintains the PCM program and PCM strategy to provide awareness of privacy risks. Assesses privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements.

(16) Reviews the Department's breach response plan (Appendix A) annually and considers whether DOE should:

(a) Update its breach response plan;

(b) Develop and implement new policies to protect the agency's PII holdings;

(c) Revise existing policies to protect the agency's PII holdings;

(d) Reinforce or improve training and awareness;

(e) Modify information sharing arrangements; and

(f) Develop or revise documentation such as System of Record Notices (SORNs), PIAs, or privacy policies.

(17) Manages privacy risks and addresses threats to privacy.

g. Chief Privacy Officer (CPO)/NNSA CPO.

(1) Manages the Enterprise Privacy Program (EPP) on behalf of the SAOP. Establishes the structure, strategic goals, objectives, and priorities of the Program, the resources dedicated, roles and responsibilities of program officials, a catalog of controls for meeting applicable privacy requirements, and any other information determined necessary by the Program.

(2) Appoints a Director of the EPP to manage daily activities.

(3) Develops and maintains Departmental privacy policies.

(4) Reviews and signs the Department's PIAs, as outlined in Attachment 2.

(5) Advises and provides subject matter expertise to the SAOP in the promulgation of guidance on privacy.

(6) Coordinates with the CIO; General Counsel (GC); NNSA Chief Privacy Officer (NNSA CPO); DOE-IN Civil Liberties and Privacy Officer; and appropriate senior officials of DEs/Sites to ensure compliance with the requirements of this Order.

(7) Manages implementation of the Department's breach response process and supports the SAOP.

(8) Serves as the SAOP's authorized designee for privacy incident response, as needed.

(9) Coordinates with the CISO, senior-level officials in the Office of the CIO, Office of the GC staff, and other stakeholder offices as appropriate, to assess and investigate reported incidents involving breaches of PII.

(10) Maintains a record of breaches of PII to include a description of the breach; steps taken to investigate the breach; an analysis of harm to privacy interests; any actions taken to mitigate potential harms or prevent similar future occurrences.

(11) Serves as the Subject Matter Expert (SME) on policy, legislation, regulations, and guidance related to information privacy.

(12) Maintains an inventory of Departmental systems containing PII on behalf of the SAOP.

(13) Ensures that Privacy Act SORNs are kept current.

(14) Uses Departmental PIAs and SORNs as resources in privacy incident response or breach investigations.

(15) Issues policies and guidance on improvements to lessen the risk of breaches of PII.

(16) Monitors implementation of activities reducing the use of SSNs and encouraging the use of encryption or other secure transmission options when sending PII through electronic means. Encourages the protection of PII both at rest and in transit within, across, and external to DOE IT systems and networks.

(17) Coordinates with the Program Manager for the DOE iJC3 and with the points of contact designated by the Secretarial Officer/Head of DE/Head of Program Office to collect and track metrics on breaches involving PII impacting the Department to respond to quarterly and annual FISMA reporting requirements.

(18) Receives and responds to privacy complaints.

h. DOE Chief Information Officer (CIO)/NNSA CIO.

(1) Advises and provides cybersecurity and information technology subject matter expertise to the SAOP and the CPO to identify ways in which the Department can safeguard privacy information.

(2) Provides current threat information regarding the compromise of PII and information systems containing PII.

(3) Ensures the SAOP and the CPO are notified of all breaches of PII within one hour of receiving notification.

(4) Ensures information systems and common controls Department-wide are covered by approved privacy plans and possess current, risk-calibrated authorizations.

(5) Partners with the CISO and CPO to ensure coordination and information sharing between enterprise information security and privacy programs.

i. DOE Chief Information Security Officer (CISO)/NNSA CISO.

(1) Partners with the SAOP and CPO to ensure coordination and information sharing between enterprise information security and privacy programs the protection of PII on Departmental information systems (in accordance with the requirements of DOE O 205.1, current version.)

(2) Advises, supports and participates in routine or situational Privacy compliance assessments of information systems that collect, use, process, or disclose Sensitive PII.

(3) Serves as a standing member of the PIRT.

(4) Coordinates with CPO to inform Office of Management and Budget, Office of Federal Chief Information Officer (OMB OFCIO) of any incidents reported to the OMB Privacy branch.

j. Privacy Incident Response Team (PIRT).

(1) Chaired and convened by the SAOP.

(2) Determines that the PII breach:

(a) Is a Major Incident, in collaboration with the SAOP; or

(b) Crosses DOE organizational boundaries.

(3) Membership includes:

(a) CPO;

(b) The CIO or the CIO's designee;

(c) The CISO;

(d) Office of the General Counsel (GC);

(e) Office of Congressional and Intergovernmental Affairs (CI);

(f) Office of Public Affairs (PA); and

(g) The DOE Program Office(s) impacted by the PII breach.

(h) The SAOP may invite other Department officials and subject matter experts as necessary to serve on the PIRT.

(4) Conducts assessments of the breach of PII, including evaluating the scope, degree of compromise, impact and risks resulting from the breach.

(5) Coordinates internal and external agency notification, including law enforcement.

(6) Serves as the Breach Response Team required by OMB M-17-12.

(7) Adds specialized members, including, but not limited to, budget and procurement personnel, human resource personnel, and/or physical security personnel, as circumstances warrant.

(8) Coordinates with the OIG to ensure significant PII breaches involving alleged or suspected crimes are reviewed for potential IG investigation.

(9) Maintains readiness for breach response activities by participating in tabletop exercises, at least annually, and completes training provided under the direction of the SAOP.

k. DE/Site CIOs and CISOs.

(1) Implement FISMA, privacy, and cybersecurity controls as required by OMB and NIST to support protection of privacy in collaboration with privacy officers.

(2) Support LPOs in responding to and investigating reported incidents and breaches involving PII.

(3) Coordinates with LPOs, along with the DOE CPO and/or NNSA CPOs, to assess Site-level privacy risks.

l. Departmental Privacy Act Officer/NNSA Privacy Act Officer.

(1) Designated by the Chief Information Officer as responsible for administering the DOE's program for implementing the requirements of the Privacy Act of 1974.

(2) Privacy Act requests for NNSA or relevant to NNSA will be transferred to the NNSA Privacy Act Officer or Local NNSA Privacy Act Officers for processing and response.

m. Local Privacy Officer (LPO).

(1) Local Privacy Officer is an umbrella term that refers to two roles: the assigned Privacy Act Officer (LPAO) and/or the Privacy Point of Contact (PPOC). Both roles are assigned by the Head of the DE/Site. Local privacy activities may require the appointment of more than one individual in each role.

(2) NNSA CPO will provide guidance through its Supplemental Guidance regarding the appointment of NNSA LPOs.

(3) Responsibilities of LPAOs include:

(a) Coordinating with the Departmental Privacy Act Officer or NNSA Privacy Officer on receipt and processing of Privacy Act requests.

(b) Coordinating with the EPP to update SORNs being used by the Program/Office/Site, as necessitated by changes in law, business process, or PII needs.

(4) Responsibilities of PPOCs include:

(a) Advocating and promoting Privacy program activities within their DEs/Sites.

(b) Serving as a liaison to the CPO, or their designee, on matters of local privacy implementation, including the facilitation of PIAs, facilitating compliance reporting, responding to data calls, assisting as needed in privacy breach response, and issues involving SORNs.

(c) Supporting the implementation of DE plans for the elimination and reduction of unnecessary uses of SSNs as an identifier.

(d) Managing the process for resolving privacy complaints for their DEs/Sites, including:

1 documentation of factual circumstances surrounding unresolved complaints; and

2 notifying the CPO of unresolved written complaints.

(e) Advising, promoting, and participating in EPP activities within their DE/Sites (including, but not limited to privacy compliance documentation, training opportunities, and routine and situational compliance reporting).

(f) Facilitating privacy control implementation, assessment and safeguarding functions related to PII for their DE/Site, including creating and maintaining privacy compliance documentation such as PTAs, PIAs, SORNs, privacy control implementation plans, incident response plans and any other needed documentation for ensuring privacy risk is managed.

n. Integrated Joint Cybersecurity Coordination Center (iJC3).

(1) Serves as the Department's Security Operations Center (SOC) for cyber incidents and privacy breaches involving Departmental IT systems and national laboratories.

(2) Coordinates with the NNSA Information Assurance Response Center (IARC) to track reported PII breaches involving NNSA sites and national laboratories.

(3) Receives reports of suspected or confirmed breaches of PII, regardless of format.

(4) Notifies CPO and the CISO of all incidents involving the breach of PII within one hour of receiving initial notification.

(5) Reports breaches of PII to the DHS Cybersecurity and Infrastructure Security Agency (CISA) in accordance with OMB directives within one hour of receiving the report of a breach.

(6) Works with the SAOP and CPO to inform the PIRT or other breach stakeholders on developments during an investigation of a breach of PII.

(7) Tracks metrics for all Departmental incidents and breaches for FISMA reporting.

(8) Provides quarterly reports to the SAOP detailing the status of each breach reported to the iJC3 during the fiscal year.

o. Senior Procurement Executive (DOE Office of Management or NNSA equivalent).

(1) Ensures that contracts include requirements regarding contractor compliance with Department or DOE Element-approved breach response plans.

(2) Works with SAOP to address deficiencies in contractor compliance with applicable privacy laws and compliance requirements.

p. Contracting Officers.

(1) Incorporate the CRD into affected contracts as directed, once notified by the affected Heads of DEs or their senior level designees regarding which contracts are subject to this Order.

(2) Ensure that contracting officers' representatives (CORs) and/or contracting officers' technical representatives (COTRs) are aware of provisions within this Order, the CRD, and any changes to their respective contracts.

(3) Ensure Privacy Act clauses contained in Federal Acquisition Regulations (FAR) at 52.224-1 and 52.224-2, and others as appropriate, are included in all solicitations and in any awarded contracts.

(4) Ensure that annual privacy training requirements for contractors are included in any awarded contracts involving business functions requiring contractors to collect, maintain, handle, or share PII.

(5) Confirm that a report of a suspected or confirmed breach of PII has been submitted to iJC3, if the contracting officer receives such a report.

(6) Consult with LPOs, DOE CPO and/or NNSA CPO, on standards for contract deliverables related to the collection, use, processing, maintenance, and sharing of PII on behalf of the Department.

q. DOE Employees.

(1) Are responsible for safeguarding PII in all forms including written, verbal, and electronic. CUI Privacy information should be sent with appropriate electronic safeguards to include encryption and password protection.

(2) Are responsible for immediately reporting suspected or confirmed breaches of PII, in printed or electronic form, in accordance with the requirements provided in Appendix A, including facilitating reporting to iJC3 and to minimize potential harm.

(3) Are responsible for complying with the Privacy Act and are aware of the risks of non-compliance with Privacy Act disclosure requirements.

(4) Cooperate with incident response teams that are investigating or attempting to resolve breaches of PII.

(5) Complete mandatory annual privacy awareness training.

r. System Owners/Data Owners.

(1) System Owners typically have budgetary oversight for the System or are responsible for the mission and/or business operations supported by the System. A contractor may serve in the role of System Owner; however, a Federal employee contact should be listed for the system on all privacy compliance documentation, including privacy impact assessments to ensure accountability.

(2) Data Owners are responsible for the selection of data elements to be collected, maintained, and disseminated within a program or system. Data Owners should be involved in the development of a system and the development of privacy compliance documentation. Data Owners should also be involved in the selection of privacy controls involving the PII collected, maintained, and disseminated within and from a System. Data Owners should be Federal employees due to the decision-making responsibilities of data ownership; however, contractors in a data management role should work with Federal Data Owners.

(3) Shared responsibilities of System Owners and Data Owners must include:

(a) Ensuring that a System collects, maintains, and disseminates only personal information considered relevant and necessary for the legally valid purpose for which it is obtained;

(b) Ensuring that, where possible, information is collected directly from the individual;

(c) Developing required privacy compliance documents and update as needed, including Privacy Act SORNs and PIAs, prior to operating a new system containing PII or making any significant change occurring to a System that affects the privacy information kept in the System;

(d) Maintaining records with accuracy, relevance, timeliness, and completeness to ensure fairness to the individual of record;

(e) Employing appropriate privacy controls for the System to protect the PII of information and to safeguard Federal records containing PII;

(f) Coordinating with LPOs to ensure appropriate privacy controls are selected, implemented, and monitored to protect PII and to safeguard Federal records containing PII.

(g) Participating in routine or situational privacy compliance assessments.

(h) Coordinating with cybersecurity, privacy, and other IT officials as needed.

s. General Counsel.

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

(2) Provides legal review and advice upon request on other privacy compliance documents.

(3) Provides legal expertise to all DOE elements in interpreting and applying privacy issues including privacy law, compliance, and training.

(4) Serves as lead on matters of law and the interpretations of law and regulations pertaining to privacy breach response.

(5) May support the implementation of the Privacy Act, including requests.

6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Note: DOE O 251.1, current version, provides a definition for "invoked technical standard."

7. DEFINITIONS. See Attachment 3.

8. REFERENCES. See Attachment 4.

9. CONTACT. Questions concerning this Order should be addressed to the DOE Chief Privacy Officer at (202) 586-0483.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

APPENDIX A
RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION

The purpose of this Appendix is to outline new responsibilities, requirements, and notification requirements impacting the Department's existing breach response procedures and processes for breaches of personally identifiable information (PII), per the requirements of Office of Management and Budget (OMB) Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, dated January 3, 2017 (M-17-12) and other subsequent governance related to cybersecurity and privacy incident response.

1. REQUIREMENTS.

   a. Reporting Breaches of PII.

      (1) Incidents or breaches affecting DOE information can occur at contractor facilities or in external locations (e.g., when an employee or contractor is on official travel, and in cloud service environments).

      (2) Upon finding a suspected or confirmed data breach of PII in printed, verbal, or electronic form, DOE employees must immediately (within one hour) report the breach using established processes to ensure it is reported:

         (a) To the LPAO and/or PPOC AND the iJC3 at 866-941-2472 (or via email to circ@jc3.doe.gov); OR

         (b) Through their DE in accordance with existing cyber incident reporting processes, which have been established in DOE Enterprise or Departmental Element Cybersecurity Program Plans (CSPPs) as defined in DOE O 205.1, Department of Energy Cyber Security Program, current version. Reports should include:

            1 The date and time of discovery of the breach;

            2 The type(s) of PII involved;

            3 Number of impacted individuals;

            4 Whether the impacted individuals are members of the public;

            5 The location of the PII (physical location, if it is spoken in conversation, or if an IT system is involved);

6 Whether the information was encrypted or secured at the time of the breach; and

7 A point of contact for follow-up questions or information gathering.

(4) The NNSA Information Assurance Response Center (IARC) must ensure that all breaches of PII are reported to the iJC3 within one hour of discovery, in accordance with DOE Order 205.1, Department of Energy Cyber Security Program, current version.

(5) Within one hour of receiving the report of a breach of PII, the iJC3 will report the breach to the Cybersecurity and Infrastructure Security Agency (CISA).

(6) The iJC3 will ensure that the CPO and the CISO are notified of all breaches of PII within one hour of receiving notification.

(7) The CPO will inform the SAOP and the CIO of the breach and work in conjunction with the iJC3 and the CISO to assess the initial impact of the breach.

(8) The SAOP and CIO, for cyber-related breaches of PII, may request assistance from senior-level officials and subject matter experts with appropriate technical and risk assessment expertise to assist the CPO's team with the initial assessment.

b. Initial Assessment of Reported Breach Involving PII.

(1) The DOE HQ Privacy Office will initiate an initial assessment of the reported breach within one business day, unless there is clear and demonstrated risk of potential harm to the affected individuals.

(2) The assessment will determine whether further technical investigation and/or risk assessment is needed to determine the impact of the breach.

(3) The assessment should examine whether mitigating factors exist that reduce the risk to the PII involved were implemented, which may result in an incident not rising to the level of a breach. Examples of mitigating factors include, but are not limited to:

(a) A phone roster containing the names and personal contact information of multiple individuals is discovered on an unsecure shared network drive. However, forensic analysis verifies that the document was only accessed by supervisors with an authorized use for that PII;

(b) A government-owned mobile device containing PII is reported lost. The PII was encrypted and the help desk was able to remotely wipe the information on the device. Forensic analysis was able to determine that the device was not accessed;

(c) An employee knowingly sends an email attachment containing their own Sensitive PII unencrypted outside of the DOE IT network; and

(d) An unsolicited email containing the purported SSNs of four individuals is received by a DOE employee. The employee realizes that the email is a spam message, reports to iJC3, and deletes the email.

(4) A finding of reasonable risk for potential misuse of involved PII will be shared IMMEDIATELY with both the SAOP and the CIO (e.g., an individual whose PII was breached by DOE reports discovering false social media accounts have been established in their name).

(5) If the SAOP and the CIO concur that the data breach does not pose a risk of substantial harm, the Department will take no further action.

(6) The SAOP will determine if the breach meets the criteria of a Major Incident.

(7) If the SAOP and the CIO (or an authorized designee) do not concur on further action, both parties will present their views to the Deputy Secretary, or designee, who will then decide what, if any, further action is necessary.

c. Escalation and Convening of the Privacy Incident Response Team (PIRT).

(1) On receiving an initial assessment report from the CPO, the SAOP will determine whether to convene the PIRT. The SAOP will chair the PIRT.

(2) The PIRT will:

(a) Determine whether additional specialized knowledge or resources will be needed to support the PIRT or the investigation, to include budget and procurement personnel, human resource personnel, law enforcement personnel, or physical security personnel;

(b) Coordinate with the OIG to ensure significant PII breaches involving alleged or suspected crimes are reviewed for potential IG investigation;

(c) Conduct and document an assessment of the risk of harm to individuals impacted or potentially impacted by the breach of PII, based on the factors outlined in internal guidance documents.

d. Individual Notification Procedures and Timelines.

(1) When breaches involve less than 1,000 affected or potentially affected individuals, the CPO and SAOP will determine whether notification is appropriate.

(2) The SAOP will advise the Secretary on whether and when to notify individuals in the event that a breach: (1) has been determined to be a Major Incident as defined by OMB; (2) impacts more than 1,000 individuals; or (3) it is otherwise determined to have a potentially significant impact to the Department. The SAOP may convene the PIRT for consultation and assistance with developing a recommended plan of action for the Secretary.

(3) The SAOP will advise the Secretary on matters including, but not limited to:

(a) Whether the Department should provide credit monitoring or identity restoration services to affected or potentially affected individuals;

(b) Which Department office or Element should have financial responsibility for the costs of breach notification and corrective services; and

(c) Whether informal, courtesy notification should be provided to OMB Privacy Branch or Congressional committees in advance of the Department providing formal notice.

(4) If notice is required, the Department will seek to provide notification to the affected or potentially affected individuals no later than ninety (90) days after the day the breach of PII was reported to iJC3. The timeline may be extended if additional information or circumstances associated with the breach require additional investigation prior to notification.

(5) If determined that an immediate and substantial risk of identity theft or other harm exists for individuals affected or potentially affected by the breach of PII, the SAOP may delegate the responsibility of providing preliminary and informal notice to affected or potentially affected individuals to the Secretarial Officer/Head of DE/Head of Program Office, or their authorized designee.

(a) Preliminary notice will be provided in accordance with the Element’s SAOP approved breach response plan.

(b) Preliminary and informal notice may be provided via an in-person meeting, by telephone, or by another appropriate alternative.

(c) Preliminary and informal notice must be followed by formal and more detailed notification once an investigation has been completed, to include cases where the investigation was extended to consider additional or new information.

(d) If notice is provided by a Departmental Element, the CPO must be notified within *24 hours* that preliminary notice has been provided and what information has been provided to the affected or potentially affected individuals.

(6) All formal notification must be approved by the SAOP and OGC (either at DOE Headquarters, NNSA OGC, or local DOE OGC, as appropriate), prior to being sent to an affected individual.

(7) Notification will not be made in instances where an individual fails to safeguard his or her own PII (*e.g.*, an employee sends his or her own PII from a government computer to his or her home email address without encryption, password protection, or secure transmission, etc.).

(8) The SAOP may delegate the responsibility for providing formal written notification to affected or potentially impacted individuals to the Head of the Departmental Element in which the breach occurred, based on: (1) the scope and impact of the breach, including the number of affected individuals; and (2) the SAOP's determination of the significance of the breach to the Department.

(9) The SAOP reserves the ability to elevate notification of an Element-based breach for handling by an appropriate Department component at his discretion.

e. Options for Corrective Services to Potentially Impacted Individuals.

(1) The Department may provide credit protection or identity restoration services to affected or potentially affected individuals based on the specific circumstances of the breach.

(2) The official authorized to determine whether to provide these services depends on the size of the breach:

(a) For breach affecting or potentially affecting less than 1,000 individuals, the SAOP will determine whether and what services will be provided.

(b) For breach affecting or potentially affecting more than 1,000 individuals, the SAOP will make recommendations to the Secretary (or his/her designee) on what services should be provided to individuals, if any.

f. Individual Notification Requirements and Methods.

(1) The SAOP and the PIRT, if convened, will advise the Secretary on the following considerations to factor into a determination on whether to notify affected or potentially affected individuals, including:

(a) The source of the notification;

(b) The timeliness of the notification;

(c) The content of the notification;

(d) The method of notification; and

(e) Any special circumstances, such as national security matters or relevant classification requirements or limitations.

(2) Criteria for Automatic Notification of Affected Persons. The SAOP will establish a process for the automatic notification of affected or potentially affected persons in the following circumstances, subject to specific guidance from law enforcement or national security officials:

(a) The impacted PII consists of Sensitive PII, such as SSNs, financial information, or health information, which has been sent unsecure via email (*i.e.*, unencrypted or sent via a secure transmission option) outside of the Department's IT network firewall; or

(b) There are clear and verifiable indications of compromise or unauthorized access to PII that could result in immediate harm to the individual by a malicious actor.

(3) Automatic notification will not be made in instances where an individual fails to safeguard his or her own Sensitive PII (*e.g.*, an employee sends a copy of a personal bank record from a government computer to his or her home email address without encryption or password protection, etc.).

(4) Automatic notification will be made under the same timelines established above.

g. Public Announcements and Media Notification.

(1) If a PIRT is not convened, then prior to the release of external announcements on the Department's main website, a DOE Element website, DOE accounts on social media platforms, or via public news statement by the Department, the SAOP will inform PA, CI, GC, the Department's White House liaison, Department officials with liaison responsibilities to White House offices, including OMB or the National Security Council (for breaches of PII with potential impacts to national security), and the President of the National Treasury Employees Union (NTEU) (other appropriate union representatives).

(2) The Department may use public announcements posted on the Department's main website or the release of a statement to the media as methods to increase outreach and awareness to affected or potentially affected individuals.

(a) Notification in print and broadcast media should include media outlets in geographic areas where the affected individuals are likely to reside, such as the locations surrounding Departmental and Element facilities.

(b) The media notice will include a toll-free telephone number or email address for an individual to use in order to learn whether his/her personal information is possibly included in the data breach.

(c) Notices posted on DOE social media accounts should include hyperlinks to a website or other information source where affected individuals can access detailed information and points of contact.

(3) Use of a public awareness campaign may also assist the Department in notifying an affected individual in cases where there may be insufficient or inaccurate contact information that has resulted in the return of written notification sent via first class mail.

h. Notification of Congress and the White House.

(1) In the event of a Major Incident, the Secretary will notify appropriate Congressional committees no later than seven (7) days after the date on which there is a reasonable basis to conclude that the breach constitutes a Major Incident.

(2) The SAOP, or the CPO as the authorized designee, will notify the Privacy Branch in OMB's Office of Information and Regulatory Affairs and will coordinate with the CISO to notify OMB's Office of the Federal Chief Information Officer, also known as the Office of E-Government and Information Technology.

i. Factors Warranting Delayed Notification of Potentially Affected Individuals.

(1) Notwithstanding the foregoing requirements, notification of affected or potentially affected individuals may be delayed on lawful requests to protect data or computer resources from further compromise or to prevent interference with the conduct of lawful investigation, national security, or efforts to recover data. Any delay should not increase risk or harm to any affected or potentially affected individuals.

(2) The Secretarial Officer, or Head of the requesting Departmental Element or Program Office will submit a written request to the SAOP regarding the need to delay notification. The request must include:

(a) An explanation of the security concern or details of the data recovery effort that may be adversely affected by providing timely notification to affected or potentially affected individuals;

(b) The lawful or authorized reason for the requested delay; and

(c) An estimated timeframe after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover data.

(3) The SAOP will submit their recommendation, along with the DOE Element's written request, to the Secretary for a final decision.

j. DOE Component/Element/Office-specific Breach Response Plan.

(1) Secretarial Officers, Heads of Departmental Elements, Heads of Program Offices, and Heads of Field Elements may elect to develop an Element-specific or site-specific breach response plan consistent with Appendix A (i.e., the Department's breach response plan), OMB Memorandum 17-12, and applicable law.

(2) Plans will be submitted for review and approval by the SAOP, with subsequent review and approval by the SAOP or his designee on an annual basis.

k. Tracking Breach Response and Notification Metrics.

(1) The CPO will collect and track metrics on breaches of PII that are submitted to the iJC3. The CPO also will track when public notification has been provided in response to a breach of PII and any other relevant metrics as determined by the SAOP.

(2) Departmental Components and their offices are required to track all activities for breaches of PII, including:

(a) Dates and times of reported breaches;

(b) Element-level decisions;

(c) Public notifications;

(d) Local corrective actions; and

(e) Any timelines for response activities. Tracking logs or spreadsheets must be submitted to the SAOP annually with a submission deadline of the end of the fiscal year (September 30).

l. Annual Readiness Requirements for Breach Response.

(1) The SAOP will convene the PIRT at least once annually to conduct privacy breach response tabletop preparedness exercises to ensure PIRT members are aware of their responsibilities and are ready to respond in the event that a PIRT is convened by the SAOP for a data breach involving PII.

(2) Ensuring systems have current privacy compliance documentation. The CPO will work with system owners to ensure that FISMA-reportable IT systems and other DOE IT systems that collect, use, store, or disseminate PII have corresponding timely and accurate privacy impact assessments and are covered by a Privacy Act SORN, if applicable.

APPENDIX B
PRIVACY ACT SYSTEM OF RECORDS (SOR) & SYSTEM OF RECORDS NOTICE (SORN) GUIDANCE

The purpose of this Appendix is to outline the requirements for the creation, maintenance, amendment, and termination of a System of Records (SOR) under the Privacy Act of 1974 (5 U.S.C. § 552a). This Appendix summarizes the requirements of Office of Management and Budget (OMB) Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication*, dated December 23, 2016 (OMB Circular A-108) and the Department's internal process for issuing or modifying a Privacy Act System of Records Notice (SORN).

1. System of Record Requirements.

   a. Information collected under the Privacy Act must be stored in a Privacy Act SOR. A SOR is 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.

   b. A SOR occurs when records are retrieved about individuals using a personal identifier, such as the individual's name or Social Security number.

   c. Privacy Act information should only be collected and maintained in Systems authorized to collect, store, and process PII.

2. Criteria for Creating a New System of Records Notice.

   a. A SORN is a formal notice published in the *Federal Register* to promote transparency by providing the public with information concerning a system of records. Details included in a SORN, as required by OMB Circular A-108, include: the purpose for the collection of information, from whom (i.e., individuals) the information is collected and what type (i.e., categories) of PII is collected, how the PII is shared external to the Department (i.e., routine uses), the safeguards that will protect the information, and how individuals may access and amend the PII maintained by the Department.

   b. The Privacy Act requires agencies to publish a SORN in the *Federal Register* and report to Congress when a new SOR is proposed, or when significant changes are made to an established system.

   c. A SORN must be in place for the following scenarios:

      (1) 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.

      (2) 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.

(3) It is discovered that records about individuals are being created and used, and that this activity is not covered by a currently published SORN.

(4) A new organization (configuration) of existing records about individuals that was not previously subject to the Privacy Act (i.e., was not a SOR) results in the need for the creation of a new SOR.

3. DOE Privacy Act SORN Process.

a. For assistance in modifying an existing SORN or creating a new SORN, please contact your local privacy officer or a member of the DOE HQ Privacy team.

b. The typical SORN development process begins with the assigned privacy officer of the DE or Site that is the primary owner of the SORN. Other stakeholders and users of the SORN will be consulted as part of the development process.

c. The DOE HQ Privacy Office will lead the development of the draft SORN package, which includes a draft SORN, a supporting narrative statement, and transmittal letters. Draft SORNs seeking a Privacy Act exemption under sections (j) or (k) of the Privacy Act will need to prepare a draft notice of proposed rulemaking as part of the draft SORN package,

d. Draft SORN packages must be submitted to Congressional committees and OMB Privacy for a 30-day review and comment period. Substantive comments from OMB and Congress may require DOE to re-submit updated drafts prior to receiving OMB or Congressional approval to process.

e. The draft SORN will be published in the Federal Register for a 30-day public comment period. If there are no public comments, the SORN is complete and usable by the Department. If public comments are received, they will be adjudicated by the Department and the Notice will be republished by the Department. Once the SORN is published in the *Federal Register*, it is subject to annual review with the primary SORN owner and the CPO.

4. What Information is Needed for a SORN? OMB Circular A-108 outlines the required components of a modification to an existing SORN, or the creation of a new SORN. In general, a SORN needs to address:

a. The authority (whether granted by statute or executive order) that authorizes the agency to solicit and collect the requested PII;

b. The principal purpose(s) for which the information is intended to be used;

c. The published routine uses which allows the agency to disclose information in specific circumstances without requiring written consent from the originating individual for each disclosure;

d. The administrative, technical, and physical safeguards in place to protect the information;

e. The means through which an individual can seek access and amend of their records under the SORN; and

f. Whether the agency is leveraging appropriate legal exemptions to limit the disclosure of certain types of information under the SORN. Agencies are allowed in certain circumstances to promulgate rules, in accordance with 5 U.S.C. § 553, to exempt a system of records from select provisions of the Privacy Act. These exemptions are outlined in Sections (j) and (k) of the Privacy Act of 1974, and usually pertain to law enforcement, national security, or active investigations.

5. Criteria for Amending a SORN.

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

b. 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 a 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.

c. Significant alterations include:

(1) 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.)

(2) 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.

(3) Change in the manner in which the records are organized, indexed, or retrieved resulting 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.

(4) Change in the purpose for which information in the system of records is used.

(5) 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.

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

This is not an exhaustive list of significant changes that would require a revised SORN. Other changes to a SOR would require a revised SORN if the changes are substantive in nature and therefore warrant additional notice.

d. 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.

e. Please consult a member of the DOE HQ Privacy team for a final determination of the nature of any changes to a system of records.

6. Rescinding a SORN.

a. When an agency stops maintaining a previously established system of records, the agency shall publish a notice of rescindment in the *Federal Register*. The notice of rescindment shall identify the system of records, explain why the SORN is being rescinded, and provide an account of what will happen to the records that were previously maintained in the system. If the records in the system of records will be combined with another system of records or maintained as part of a new system of records, the notice of rescindment shall direct members of the public to the SORN for the system that will include the relevant records.

b. There are many reasons why agencies may need to rescind a SORN. For example, the Privacy Act provides that an agency may only collect or maintain in its records information about individuals that is relevant and necessary to accomplish a purpose that is required by statute or executive order. If a system of records is comprised of records that no longer meet that standard, the Privacy Act may require that the agency stop maintaining the system and expunge the records in accordance with the requirements in the SORN and the applicable records retention or disposition schedule approved by the National Archives and Records Administration (NARA).

c. For assistance in rescinding an existing SORN, please contact your local privacy officer or a member of the DOE HQ Privacy team.

7. Privacy Act Exemption Rules.

a. The Privacy Act includes two sets of provisions that allow agencies to claim exemptions from certain requirements in the statute. These provisions allow agencies in certain circumstances to promulgate rules, in accordance with 5 U.S.C. § 553, to exempt a system of records from select provisions of the Privacy Act.

b. Generally, these procedures will require agencies to publish in the *Federal Register* a proposed rule soliciting comments from the public, followed by a final rule. At a minimum, agencies' Privacy Act exemption rules shall include:

(1) The specific name(s) of any system(s) that will be exempt pursuant to the rule (the name(s) shall be the same as the name(s) given in the relevant SORN(s));

(2) The specific provisions of the Privacy Act from which the system(s) of records is to be exempted and the reasons for the exemption (a separate reason need not be stated for each provision from which a system is being exempted, where a single explanation will serve to explain the entire exemption); and

(3) An explanation for why the exemption is both necessary and appropriate.

c. When agencies wish to promulgate a Privacy Act exemption rule, agencies shall submit the draft rule to OMB along with the new or revised SORN(s) associated with the systems that the agency wishes to exempt, so that OMB can review the proposed exemption rule along with the SORN.

d. For assistance with Privacy Act exemptions and the required rulemaking process for exemptions, please contact your local privacy officer or a member of the DOE HQ Privacy team.

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 206.1A, *DEPARTMENT OF ENERGY PRIVACY PROGRAM*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) site/facility management contractors whose contracts involve the collection, use, processing, maintenance, management, handling, sharing, dissemination, or disposal of Personally Identifiable Information (PII) on behalf of the DOE. This includes contractors responsible for the development or operation of information held in a government-wide or DOE Privacy Act System of Record. Please review the definitions for "Federal information system" and "contractor information system" found in Appendix 3, which should be used to determine applicability for this CRD. Federal information does not include information that is defined to be information owned by the contractor pursuant to 48 C.F.R. 5204-3, *Access to and Ownership of Records*, as provided in each contract.

Regardless of the performer of the work, the contractor organization is responsible for ensuring their employees comply with the requirements of this CRD. The contractor organization is also responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's or subcontractor's compliance with the requirements.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachments 2, 3, and 4, referenced in and made a part of this CRD, which provide program requirements and/or information applicable to contracts in which this CRD is inserted.

1. GENERAL REQUIREMENTS. Contractor organizations must:

   a. Establish processes to ensure contractor employee compliance with applicable privacy laws and requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, the privacy protection standards implemented by the National Institute of Standards and Technology, and associated Office of Management and Budget (OMB) directives.

   b. Ensure that contractor employees:

      (1) Receive annual training on privacy, including their responsibilities to safeguard PII;

      (2) Report suspected or confirmed breaches of PII to DOE in accordance with DOE O 205.1, current version and Appendix A of DOE O 206.1A; and

      (3) Comply with the requirements of the Privacy Act.

   c. Ensure PII and Privacy Act information, in any format, electronic or hard copy, is protected and secured, marked, and disposed of when no longer required in accordance with applicable orders with records disposition schedules.

d. Appoint a Privacy Representative, as appropriate to:

(1) Ensure that PII and Privacy Act information, as defined in DOE O 206.1A, in any format, is protected and secured;

(2) Oversee local privacy development, implementation, and performance reporting activities;

(3) Support contractor employees responsible for developing privacy compliance documents, including privacy impact assessments; and

e. Contractor organizations must also comply with all applicable and appropriate privacy- and security-related clauses as outlined in the Federal Acquisition Regulations (FAR), DOE's Acquisition Regulations (DEAR), and specific requirements included in blanket purchase agreements (BPAs) and M&O contracts.

2. SPECIFIC REQUIREMENTS. At a minimum, contractor organizations must ensure contractor employees:

a. Do not disclose any PII contained in a Privacy Act System of Record except as authorized.

b. Report any suspected or confirmed breach of PII involving Federal information within one hour, consistent with the agency's breach response procedures outlined in DOE O 206.1A and DHS CISA breach notification guidelines.

c. Assist with the investigation and mitigation of harm (e.g., including but not limited to: coordinating removal of messaging and files containing unauthorized, compromised, or exposed PII within the IT system; sending notifications to affected individuals; providing the option of credit monitoring; and other appropriate measures) following a breach of PII involving Federal information under the custody of the contractor.

d. Observe the requirements of DOE directives concerning marking and safeguarding sensitive information, including, when applicable, DOE O 471.7, *Controlled Unclassified Information,* current version.

e. Collect only the minimum PII necessary for the proper performance of a documented contract function or deliverable.

f. Ensure that PII placed on shared drives, intranets, cloud networks, or websites is in accordance with appropriate security and privacy controls and contract requirements for safeguarding information.

g. Support DOE in the implementation of Section 208 of the E-Government Act of 2002. System Owners and Data Owners are responsible for developing and maintaining privacy compliance documentation for systems involving PII[2] in accordance with Attachment 2 to DOE O 206.1A.

h. Recognize that non-compliance with the Privacy Act carries criminal and civil penalties.

i. Allow and cooperate with inspection or investigation to determine compliance with this CRD.

j. Complete annual mandatory privacy awareness training and any role-based training required to access or perform jobs involving PII.

[2] System refers to Federal Information Systems and Contractor Information Systems, as defined in Attachment 3 of this Order.

ATTACHMENT 2
DOE PRIVACY IMPACT ASSESSMENT PROCEDURES

This Attachment provides information and/or requirements associated with DOE O 206.1A as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 206.1A) is inserted.

NNSA and DOE-IN will issue supplemental guidance for Privacy Impact Assessments (PIAs) for Systems under their control and purview including National Security Systems (NSS). For DOE-IN NSS, System Owners shall work with DOE-IN's Office of Civil Liberties and Privacy to develop PIAs for these Systems. For NNSA NSS, System Owners shall work with NNSA's Chief Privacy Officer to develop PIAs for these Systems.

1. Requirements to Conduct Privacy Impact Assessments (PIAs).

   a. Section 208 of the E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) in order: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, using, and disseminating personally identifiable information (PII) about individuals for business purposes, (iii) to assist the Department in assessing the amount of PII held within information collections and electronic information systems, and (iv) to mitigate potential privacy risks through examining and evaluating protections and alternative processes for handling information.[1]

   b. A PIA is a documented snapshot of the privacy impacts and risks assumed by the Program/Office/Site in operating an IT system or business use that requires PII. It seeks to ensure System consideration of and compliance with the Fair Information Privacy Principles (FIPPs) of accountability and auditing, data minimization, data quality, individual participation, purpose specification, security, transparency, and use limitation. The Department of Energy (DOE) PIA process ensures privacy protections are considered and implemented throughout the System[2] lifecycle.

   c. While this Attachment is focused on PIA requirements for Systems, the SAOP and CPO reserve the right to require the development of PTAs and PIAs for operational Programs or Projects with privacy implications that warrant that the Department provides transparency into these activities.

---

[1] Other legal requirements for the conduction of PIAs include Section 522 of the 2005 Consolidated Appropriations Act, Appendix II of OMB Circular A-130, *Managing Information as a Strategic Resource*, and OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications.*

[2] System refers to Federal Information Systems and Contractor Information Systems, as defined in Attachment 3 of this Order.

2. Who Participates in the PIA Process?

a. The development and maintenance of a PIA is a responsibility of the System Owner. The System Owner has the central role in privacy compliance development and should ensure that local stakeholders are aware and engaged at the appropriate steps of the PIA process, but the System Owner, Data Owners, and the Local Privacy Officer must work together to complete the PIA.

b. Data Owners must identify data that is collected and maintained in the information system, as well as individuals who will access that data.

c. The Local Privacy Officer, in collaboration with DOE HQ Privacy, must determine whether there are any potential risks to privacy. They must maintain copies of approved PTAs and PIAs for the Program/Office/Site to ensure their awareness of PII holdings and the Program/Office/Site's acceptance of privacy risks in authorized Systems. DOE HQ Privacy will communicate with System Owners and LPOs during the review of the PTA to include providing estimated completion timelines.

d. PIAs require collaboration with program experts as well as experts in the areas of information technology, cybersecurity, records management, and privacy. Other resources may include:

(1) Legal counsel, when pointing to specific legal authority that permit the collection of PII for the business purpose.

(2) Records Officers, for identifying records and disposition authorities.

(3) Security Officers, to provide System security documents to augment PIA narratives.

(4) Operational partners, to ensure that related PIAs also address PII exchanges and uses between systems.

(5) DOE HQ Privacy Office, to conduct analysis of documented privacy risks.

(6) Chief Privacy Officer, to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.

3. What Triggers the DOE PIA Process for a System**?**

a. An important note: the PIA process must be conducted and approved before PII is collected for use by a program. Proactive engagement of privacy professionals during the planning and development stages of a system or project will enable privacy to be managed and documentation to be developed.

b. Before beginning the PIA process, the Data Owner or System Owner must determine whether PII or other information pertaining to privacy interests is required to be collected, maintained, used, or shared to support authorized business or mission needs.

c. The determination of whether PII or other information pertaining to privacy interests is required to be collected, maintained, used, or shared is a mandatory first step for all unclassified information systems, including contractor systems operated for or on behalf of DOE.

(1) If the answer is yes (PII is required for the System's business purpose), the System Owner should initiate the privacy compliance process outlined below, in collaboration with the Data Owner, local privacy and security personnel, and any other necessary stakeholders.

(2) If the answer is no, and PII is not required for a business purpose to be collected, maintained, used, or shared by the System, the DOE PIA process is not applicable, and no further documentation is required.

4. Navigating the PIA Process. DOE has devised a multi-step system overseeing each stage of the PIA lifecycle: initial analysis, document development, analytical review and approval, substantive updates, annual reviews, and decommissioning/disposal due to the end of the lifecycle of PII within the System.

a. Document Development: Privacy Threshold Assessment.

(1) The Privacy Threshold Assessment (PTA) should be completed by a System Owner as early as possible, but in all cases before implementing that System. The PTA identifies whether the System will collect and maintain PII, and whether additional privacy compliance documentation, such as a PIA or system of records notice (SORN) is required.

(2) Using the resources listed above in "Who Participates in the PIA Process?", the System Owner, in collaboration with their Local Privacy Officer, will answer the PTA's threshold questions to determine if, and to what extent, their System collects, maintains, or disseminates information in identifiable form. Based on the context of the PII in the System and the privacy risk it poses to individuals as documented in the PTA, the System Owner and Local Privacy Officer will recommend a path forward of compliance documentation for the System in question. Possible recommendations include:

(a) If no PII or only system administrative PII is present (i.e., PII to validate user identity or authorize access, not used for another business purpose), then the completed PTA itself is sufficient.

(b) If PII is present but represents manageable risk of harm to individuals and is not being used in a context that raises the risk level, the Local System Owner will be instructed to complete a Short Form PIA.

(c) If PII is present and the context and risk meet the definition of Sensitive PII, the System Owner will be prompted to complete a Full PIA to DOE HQ Privacy.

(3) Once the System Owner and LPO have completed the PTA, they shall send it to the DOE HQ Privacy Office for concurrence on the recommendation. DOE HQ Privacy may determine that additional documentation is needed beyond the LPO's recommendation and will communicate that determination to the LPO and System Owner in a time-bound manner.

(4) Once DOE HQ Privacy has concurred with the recommendation of completing only a PTA for the System, the PTA will be certified by a member of the DOE HQ Privacy team and no further action will be required by the System Owner or LPO until the System's Annual Review. This includes PTAs for Systems with no PII or only system administrative PII.

b. Document Development: Privacy Impact Assessment.

(1) If the PTA determines that further documentation is needed, the System Owner will complete either a Short Form PIA or Full PIA commensurate with the level of privacy risk as identified through the PTA.

(2) Privacy, like security, should be considered at all stages of the system's lifecycle (i.e., collection, use, retention, processing, disclosure, and destruction). At a minimum, PIAs must be conducted when:

(a) Designing, developing, or procuring information systems or IT projects that collect, maintain, or disseminate PII.

(b) Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of PII for 10 or more persons.

(c) Identifying a business process or mission need requiring the collection, use, and sharing of PII.

(3) The PIA is designed to be more in-depth than the PTA. A PIA's questions mirror the FIPPs mentioned previously.

c. Short Form PIA.

(1) Non-Sensitive PII or privacy concerns require the drafting of a Short Form PIA. The purpose of the Short Form PIA is to provide transparency into the business need for the PII and how it will be used and protected by DOE and its contractors.

(2) Situations warranting a Short Form PIA may include, but are not limited to:

(a) The organization collects names and email addresses from the public to sign up interested individuals to receive a periodic newsletter or informational emails.

(b) An email inbox is set-up to receive resumes submitted from members of the public. The mailbox is only used to collect resumes, but communication with applicants occurs through other established business processes.

(3) Once the PTA's recommendation of completing a Short Form PIA has been accepted by DOE HQ Privacy, the System Owner and LPO will complete a Short Form PIA and certify locally. The CPO does not need to sign these documents for them to be considered official, but local Sites should keep copies in case of a Headquarters Audit. Sites will send signed copies of signed Short Form PIAs to DOE HQ Privacy to comply with requirements regarding PIA publication.

d. Full PIA.

(1) Full PIAs outline the risks associated with Sensitive PII concerns, combinations of PII that create an increased risk of harm to individuals, or Systems that require additional scrutiny.

(2) Examples of situations that may result in the development of a Full PIA include but are not limited to:

(a) If the System collects, uses, maintains, or disseminates financial information, medical information, or Social Security numbers.

(b) If the System is classified as a DOE "High Value Asset."

(c) If the System collects PII in combination with other sensitive or special marked information (determined in consultation with DOE HQ Privacy or appropriate alternative roles in DOE-IN and NNSA).

(d) If the System is part of a reportable FISMA security enclave, and collects Sensitive PII.

(e) Any other context in which the risk threshold meets the definition of Sensitive PII, as determined by this Order or guidance issued by DOE HQ Privacy.

(3) Once the PTA's recommendation of completing a Full PIA has been accepted by DOE HQ Privacy, the System Owner/LPO will complete a Full PIA and liaise with DOE HQ Privacy until all outstanding questions have been addressed satisfactorily. The CPO will sign and ask the Local Site to maintain a copy in case of audit.

e. PIA Publication.

(1) PIAs are publicly releasable documents. Per the requirements of section 208 of the E-Government Act, the Department's PIAs will be made available through a public-facing repository on DOE's Privacy website (energy.gov/privacy).

(2) PIAs that contain proprietary information or pertain to classified information systems will be conducted but will not be made publicly releasable. If these PIAs must be released, the System Owner shall work with DOE HQ Privacy to prepare a redacted version for publication.

(3) PIAs for National Security Systems or Systems containing information protected by law such as Controlled Unclassified Information (CUI) and Unclassified Controlled Nuclear Information (UCNI) will not be made publicly available.

f. Substantive Updates. In short, PIAs should be updated whenever there is a change to the information system that affects privacy or creates new risks to privacy. These changes can be grouped into the following broad categories:

(1) New collection of information that is linked or linkable to individuals.

(2) Significant changes, including those that affect:

(a) How existing information that is linked or linkable to individuals is managed internally (e.g., significant system management changes, significant merging, internal flow or collection, changes to business processes or authorities collecting the information, etc.); or

(b) How existing information that is linked or linkable to individuals is managed externally (e.g., incorporating data from commercial or public sources, new interagency uses, etc.); or

(c) Access of existing information that is linked or linkable to individuals (e.g., converting paper-based records to electronic systems, new public access, etc.); or

(d) The risk level of existing data (e.g., changing anonymous information to non-anonymous, other alteration of character in data, etc.).

g. Annual Reviews and Decommissioning of Systems with PII.

(1) All PTAs and PIAs shall be reviewed by System Owners at least annually. Annual Reviews are critical to identifying the need for substantive updates to PTAs and PIAs (see above).

(a) System Owners must submit an Annual Review Summary for each System with an approved PTA/PIA to the Local Privacy Officer and DOE HQ Privacy.

(b) Minor administrative changes such as personnel changes from those documented in the original PTA or PIA will be captured in the Annual Review Summary.

(2) For Systems with PII that are scheduled to be decommissioned, the System Owner will work with DOE HQ Privacy to document the disposal of PII maintained within the System and to update existing compliance documents to reflect the changed status of the System.

ATTACHMENT 3. DEFINITIONS

This Attachment provides information associated with DOE O 206.1A as well as information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 206.1A) is inserted.

1. Breach or Data Breach.[1]

   a. An incident involving the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

      (1) A person other than an authorized user accesses or potentially accesses PII; or

      (2) An authorized user accesses or potentially accesses PII for other than the authorized purpose.

   b. Breaches *do not* require evidence of harm to an individual, or of unauthorized modification, deletion, exfiltration, or access to information.

   c. PII can be breached in any format, including physical (paper), electronic, and verbal/oral.

   d. A determination of whether a breach occurred is dependent on the availability of facts and circumstances; thus, the determination may occur at any time and any disposition of breach status is not necessarily final.

   e. The Elements of a Breach are further defined as follows:

      (1) Unauthorized modification is the act or process of changing components of information and/or information systems.

      (2) Unauthorized deletion is the act or process of removing information from an information system.

      (3) Unauthorized exfiltration is the act or process of obtaining—without authorization or in excess of authorized access—information from an information system without modifying or deleting it.

      (4) Unauthorized access is the act or process of logical or physical access without permission to a Federal agency information system, application, or other resource.

[1] These definitions of "Incident," "Breach," and "Major Incident" are consistent with the definitions established in OMB M-17-12, and OMB's annual fiscal year *Guidance on Federal Information Security and Privacy Management Requirements* and may differ from similar definitions used in existing Department Orders, Directives, Memoranda, or other policy documents. For the purpose of privacy incident response, this version of the definition will guide Departmental action and response.

f. Examples of breaches that must be reported include, but are not limited to the following:

(1) Loss of control or similar occurrence (e.g., unencrypted email or not using a secure method of transmission) of Sensitive DOE employee or contractor PII;

(2) Loss of control or similar occurrence of Department credit card holder information;

(3) Loss of control or similar occurrence of PII collected from or pertaining to members of the public;

(4) Loss of control or similar occurrence of system security information (e.g., username, passwords, security question responses, etc.);

(5) Incorrect delivery of PII to an unauthorized person;

(6) Theft of or compromise of PII; or

(7) Unauthorized access to PII stored on Department-managed information systems or managed for the Department, including websites, data centers, cloud services, etc.

For these purposes, reportable PII does not include common business exchanges such as names and/or business contact information.

g. Examples of breaches of PII include, but are not limited to:

(1) A laptop or removable storage device containing PII is lost or stolen and information on the device is accessed;

(2) An employee or contractor's system access credentials are lost or stolen to gain access to files containing PII;

(3) An unencrypted email containing Sensitive PII is sent to the wrong person, inside or outside of the Department email network;

(4) Files or documents with PII, such as medical information, are lost or stolen during shipping, courier transportation, or relocation;

(5) PII is posted, either inadvertently or with malicious intent, to a public website or can be accessed through a Departmental-operated web page or website;

(6) An unauthorized person overhears Departmental employees or contractors discussing the PII of another individual; or

(7) An IT system that collects, maintains, or disseminates PII is accessed or compromised by an unauthorized person or malicious actor.

2. Contractor. For purposes of the Directives Program, organizations under contract with DOE to perform services with the clause at DEAR 970.5204-2, Laws, Regulations and DOE Directives, in their contracts or requiring incorporation of a CRD in their contracts to implement an Order.

   At DOE, this definition of contractor does not include all of the procurement contracts entered into by DOE.

3. Contractor Information System. An information system used or operated by a contractor of the Department, including M&O contractors, to generate, acquire, manage, process, and store information that is owned by the contractor as defined in the contract.

4. Data Quality. Ensuring, within sufficient tolerance for error, the quality of the record in terms of its use in making a decision or determination which will affect an individual. It is recommended that information be collected directly from the individual to ensure the accuracy, relevance, and timeliness of the data.

5. Fair Information Practice Principles (FIPPs). The foundational principles for privacy policy and guideposts for an organization's implementation of privacy protections and management of PII. The eight DOE FIPPs are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability/Auditing.

6. Federal Information. Information that is created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form (as defined by OMB Circular A-130).

   At DOE, Federal Information may include information collected by a contractor at the direction of a Federal mandate or contract clause. Federal information does not include information that is defined to be information owned by the contractor pursuant to 48 C.F.R. 5204-3, Access to and Ownership of Records, as provided in each contract.

7. Federal Information System. An information system used or operated by the Department or by a contractor of an agency or by a contractor or other organization on behalf of the Department (as defined by OMB A-130).

   a. At DOE, Federal Information System includes systems operated by the DOE or by contractors on behalf of the DOE where the system is used to accomplish a Federal function.

   b. Federal Information Systems do not include systems operated by M&O contractors that meet the definition of a Contractor Information System.

8. Incident.[2] 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.

   This Order and its Appendices and Attachments use the term "incident" as the broader term for a situation involving information or information systems. Not all incidents are breaches.

9. Major Incident.[3] A breach constitutes a "Major Incident" when either:

   a. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.[4] Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide, OR,

   b. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.[5]

      In terms of a numeric threshold, the DOE SAOP will consider the character of the PII and the circumstances of the breach in making this determination, particularly where Sensitive PII (as defined below) is involved. Accordingly, in some instances breaches impacting fewer than 100,000 individuals may constitute a Major Incident. Additionally, breaches of Sensitive PII of individuals approaching

[2] See footnote 1 in this Attachment.

[3] See footnote 1 in this Attachment.

[4] Using the CISA Cyber Incident Scoring System, this includes Level 3 events (orange), defined as those that are "likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence"; Level 4 events (red), defined as those that are "likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties"; and Level 5 events (black), defined as those that "pose an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons."

[5] The analysis for reporting a major breach to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach. When assessing the potential risk of harm to individuals, agencies should refer to OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017).

or exceeding the 100,000 individual threshold may be a Major Incident even if there is no direct evidence of unauthorized access, deletion, or access.

10. National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which:

    a. Involves intelligence activities;

    b. Involves cryptologic activities related to national security;

    c. Involves command and control of military forces;

    d. Involves equipment that is an integral part of a weapon or weapons system;

    e. Is critical to the direct fulfillment of military or intelligence missions, not including systems that are to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

    f. Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

11. Non-Sensitive PII. See definition of "Personally Identifiable Information (PII)."

12. 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**. PII can include unique individual identifiers or combinations of identifiers, such as an individual's name, Social Security number, date and place of birth, mother's maiden name, biometric data, etc. (as defined by OMB Circular A-130).

    PII is determined by the ability of the information or data element to be used to identify an individual. Context can change whether a data element should be labeled as PII. Some PII may present a higher risk to an individual because of its use in other business or financial processes.

    At DOE, for the purposes of privacy compliance documentation (i.e., PTAs and PIAs), PII will be assessed in terms of "Non-Sensitive" and "Sensitive" PII.

    Sensitive PII is defined for compliance purposes as "Personally Identifiable Information, which if lost, compromised, or disclosed with or without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised." This includes circumstances in which a minimal amount of PII is provided in a context that increases the sensitivity and/or risk

of harm to an individual. For example, a list of names of employees with whistleblower status would be considered more sensitive than a simple roster of employee names.

Non-Sensitive PII is "Personally Identifiable Information that represents manageable risk of harm to individuals and is not being used in a context that raises the level of sensitivity." Non-Sensitive PII would include PII that is used for the administration of Systems, such as work email address, username, passwords, or security verification questions. Some Non-Sensitive PII may warrant additional protections regardless of its Non-Sensitive status. For example, Personal PII should always be treated with greater sensitivity than work-related PII to retain the trust of the individual.

PII definitions related to Breaches, Data Breaches, and Incidents involving PII should follow the definitions for "Breach or Data Breaches" and "Incident" included in this Attachment in terms of defining the circumstances and sensitivity of PII involved for the purposes of reporting and responding to suspected or confirmed incidents or breaches involving PII.

13. Privacy Act Information. Information that is required to be protected under the Privacy Act of 1974. Information subject to the Privacy Act must be retrieved by a unique personal identifier, such as a name or unique identification number or code. Privacy Act information must be safeguarded and handled in accordance with the requirements and restrictions outlined in the Privacy Act. Any grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger- and voice print or a photograph is considered a record for the purposes of the Privacy Act.

14. Privacy Act Request. A request to an agency to gain access to an individual's record, such as by another Federal agency or law enforcement as required by statute; a request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system.

15. Privacy Compliance Documentation. See entries for Privacy Threshold Assessment and Privacy Impact Assessment.

16. Privacy Control. An administrative, technical, or physical safeguard, as defined by NIST guidance, implemented within information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Selected controls ensure compliance with applicable privacy requirements, manage privacy risks, and must be documented, monitored, and periodically assessed for continued effectiveness.

17. Privacy Impact Assessment (PIA). A documented analysis of how information is handled to:

    a. Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

b. Determine the risks and effects of collecting, maintaining and disseminating PII in an electronic information system or information collection; and

c. Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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

19. 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.

20. Sensitive PII (SPII). See definition of "Personally Identifiable Information (PII)."

21. System of Records (Privacy Act). 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. The responsible component for each Privacy Act SOR is listed as the System Manager in the published notice.

22. System of Records Notice (SORN). Notice published in the *Federal Register* prior to an agency's collection, maintenance, use or dissemination of information about an individual.

ATTACHMENT 4. REFERENCES

1. Federal Laws and Regulations.

   a. Privacy Act of 1974, as amended at 5 U.S.C. §552a.

   b. E-Government Act of 2002, Public Law 107-347.

   c. Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq*.

   d. Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283.

   e. Social Security Number Fraud Prevention Act of 2017, Public Law 115-59.

   f. DOE Privacy Act Regulation, 10 CFR Part 1008.

   g. The Freedom of Information Act (FOIA), 5 U.S.C. §552.

   h. DOE FOIA Regulations, 10 CFR Part 1004.

   i. Federal Acquisition Regulations (FAR).

   j. Department of Energy Acquisition Regulations (DEAR).

   k. Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES), Public Law 116-50.

   l. 21st Century Integrated Digital Experience Act (IDEA) of 2019, Public Law 115-336 (21st Century IDEA Act).

2. Executive Orders.

   a. Executive Order 13719, Establishment of the Federal Privacy Council (February 09, 2016).

   b. Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021).

3. Office of Management and Budget (OMB) Circulars and Memoranda.

   a. OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act.

   b. OMB Circular A-130, Managing Information as a Strategic Resource.

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

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

e. OMB Memoranda on Federal Information Security and Privacy Management Requirements, issued annually by fiscal year.

f. OMB M-21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act.

4. National Institutes of Standards and Technology (NIST).

a. NIST Privacy Framework, current version.

b. NIST Special Publication (SP) 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, current version.

c. NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, current version.

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

5. Department of Energy Directives.

a. DOE P 205.1, *Departmental Cyber Security Management Policy*, current version.

b. DOE O 200.2, *Information Collection Management Program*, current version.

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

d. DOE O 221.1, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*, current version.

e. DOE O 221.2, *Cooperation with the Office of Inspector General*, current version.

f. DOE O 243.1, *Records Management Program*, current version.

g. DOE O 331.1, *Administering Work Force Discipline, Adverse, and Performance Based Actions*, current version.

h. DOE O 471.7, *Controlled Unclassified Information*, current version.