U.S. Department of Energy
Washington, DC

ORDER

DOE O 206.1

Approved: 1-16-2009
Chg 1 (MinChg): 11-1-2018

SUBJECT: DEPARTMENT OF ENERGY PRIVACY PROGRAM

1. PURPOSE.

   a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E-Government Act of 2002, and associated Office of Management and Budget (OMB) directives.

   b. Establish a Departmental training and awareness program for all DOE Federal and contractor employees to ensure personnel are cognizant of their responsibilities for—

      (1) safeguarding Personally Identifiable Information (PII) and

      (2) complying with the Privacy Act.

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

2. CANCELS/SUPERSEDES. DOE O 206.1, *Department of Energy Privacy Program*, dated 01-16-09, 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or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.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. DOE Elements. Except for the exclusions in paragraph 3.c., this Order applies to all Departmental Elements, including those created after the Order is issued.

      The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this Order.

   b. DOE Contractors. Except for the exclusions in paragraph 3.c., the CRD (Attachment 1) sets forth contractor requirements. The CRD will apply to the extent set forth in each contract.

   c. Exclusions.

      (1) In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511, and

to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Order for activities under the Director's cognizance, as deemed appropriate.

(2) Nothing in this Order shall be construed to provide any employee of DOE who is not an employee of the National Nuclear Security Administration (NNSA), other than the Secretary and Deputy Secretary, authority, direction or control of any employee or contractor of NNSA. The Administrator of NNSA will assure that NNSA employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under Section 3212(d) of Public Law (P.L.) 106-65 to establish NNSA-specific policies, unless disapproved by the Secretary.

4. REQUIREMENTS. The following privacy requirements apply to all Departmental Elements.

a. Safeguarding Personally Identifiable Information (PII).

(1) OMB has defined PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

(2) Employees are required to prevent the unauthorized breach of PII.

(3) Upon a finding of a suspected or confirmed data breach of PII in printed, verbal, or electronic form, DOE employees must ensure that the breach is IMMEDIATELY reported:

(a) to both the local Privacy Act Officer (PAO) and/or Privacy Point of Contact (PPOC) AND to the Integrated Joint Cybersecurity Command Center (iJC3) at 866-941-2472 (or via email to circ@jc3.doe.gov); OR

(b) through their Departmental Element in accordance with existing cyber incident reporting processes, which have been established in Senior DOE Management Program Cyber Security Plans (PCSPs) as defined in DOE O 205.1, Department of Energy Cyber Security Program, current version.

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

(5) DOE employees shall limit the use of PII to only that information which is specifically needed to carry out their duties.

b. The Privacy Act. The Privacy Act governs a Federal agency's ability to maintain, collect, use, or disseminate a record about an individual.

(2) 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 or voice print or a photograph is considered a record for the purposes of the Privacy Act.

(3) The Privacy Act allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President.

(4) Information collected under the Privacy Act must be stored in a Privacy Act System of Records (SOR).

(5) A SOR has the following two key distinctions:

(a) an indexing or retrieval capability built into the system and

(b) the Department retrieves records about individuals by reference to a personal identifier, such as the individual's name or Social Security number.

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

(7) Each SORN must contain the following information:

(a) name and location of the system;

(b) categories of individuals on whom records are maintained in the system;

(c) categories of records maintained in the system;

(d) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(e) policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(f) title and business address of the agency official who is responsible for SOR;

(g) agency procedures whereby an individual can be notified at the individual's request if the SOR contains a record pertaining to the individual; and

(h) agency procedures whereby an individual can be notified at the individual's request how he/she can gain access to any record pertaining to him/her contained in the SOR, and how he/she can contest its content; and categories of sources of records in the system.

(8) Under the Privacy Act, with limited exceptions, no agency or person shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

(9) For each SOR, DOE must not permit information collected about an individual for one purpose to be used for another purpose without giving notice to or getting the consent of the subject of the record and unless the record is being used subject to a routine use.

(10) Non-compliance with the Privacy Act carries **criminal and civil** penalties. An employee may be liable if he or she knowingly and willfully—

(a) obtains or requests records under false pretenses,

(b) discloses privacy data to any person not entitled to access, or

(c) maintains a "system of records" without meeting Federal Register notice requirements.

(11) Recognizing differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, employees must be cognizant that these are two separate authorities that impose different responsibilities on federal employees and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act. PII not maintained in a Privacy Act SOR should be protected and only disclosed for authorized purposes.

(12) DOE employees must receive yearly training on privacy and data protection policies.

(13) Privacy Impact Assessment. All unclassified information systems shall have a Privacy Impact Assessment (PIA) approved by the Senior Agency Official for Privacy (SAOP) or designated official. PIAs must be reviewed and updated at least annually (see Appendix A).

(14) Collection and use of Social Security numbers. Collection and use of Social Security numbers not required by statute, regulation or an intended Departmental purpose shall be eliminated, in practice and in form, from DOE information systems and programs, whether in electronic or paper media.

(15) Senior DOE Management, as defined in DOE O 205.1, *Department of Energy Cyber Security Program*, current version, may add to these requirements for their own organizations, based on assessment of risk, so long as any additional direction is consistent with these requirements.

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), which will include, at a minimum:

(a) The Department's SAOP;

(b) the Department's Chief Privacy Officer (CPO);

(c) the Chief Information Officer (CIO) or the CIO's designee;

(d) the Chief Information Security Officer (CISO);

(e) a senior official from the Office of the General Counsel (GC);

(f) the Office of Congressional and Intergovernmental Affairs (CI); and

(g) the Office of Public Affairs (PA).

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

(3) Makes a final decision on whether the Department will provide notification.

(4) Makes a determination on whether additional identity protection services will be provided to individuals affected by a breach involving PII.

(5) Determines which Department Office or Element is responsible for covering the financial costs of notification and corrective services, if needed. Generally, this will be the Office or Element responsible for the breach.

(6) Reports breaches that the SAOP 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.

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/Heads of Program Offices/Heads of Field Offices.

(1) Have responsibility and accountability for ensuring the Departmental Elements' implementation of privacy protections in accordance with Federal laws, regulations, Departmental policies and Directives.

(2) Ensure completion of PIAs of all unclassified information systems within their purview, including systems that only collect or maintain information about DOE employees and DOE contractors, in accordance with the requirements of this Order and all appendices.

(3) At a minimum, Departmental Elements must implement the following safeguards:

(a) Implement Cyber Security Controls outlined in DOE Directives and CIO guidance for the protection of PII.

(b) Ensure all individuals with authorized access to PII and their supervisors sign at least annually a document clearly describing their responsibilities.

(c) Ensure personnel minimize the collection of PII to only that which is required to conduct business operations necessary for the proper performance of a documented DOE function.

(d) Identify systems that process PII and ensure access is limited to only those individuals whose work requires access.

(e) Use sealable, opaque envelopes for mailing PII. Mark envelope to the person's attention.

(4) Post privacy policy statements on DOE websites in accordance with Federal law, regulations, and OMB directives.

(5) Appoint site Privacy Act Officers or points of contact for their Departmental Elements.

(6) Implement their Elements' plans to eliminate the unnecessary collection and use of Social Security numbers.

(7) 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, DOE Elements or Offices, or DOE IT systems or networks.

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

(9) If applicable, support the SAOP and the CPO in conducting annual reviews of the Element's or Program Office's privacy incident response plans and periodic audits of Element's or Program Office's breach response activities.

(10) Ensure that all Element or Program Office 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 Element or Program Office site will provide tracking reports to the SAOP on request.

(11) Ensure that breaches involving PII in any form—written, electronic, or verbal—are reported to both the Department's Integrated Joint Cybersecurity Coordination Center (iJC3) and the SAOP IMMEDIATELY.

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

d. Senior Agency Official for Privacy (SAOP).

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

(2) Oversees Departmental response to breaches involving PII.

(3) 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, with the exception of decisions related to the Department's response to a Major Incident.

(4) Determines whether a breach meets the criteria of a Major Incident.

(5) Determines whether a breach of PII reported by an Element or Program Office 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.

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

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

(8) 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 identify restoration services.

(9) Reviews and approves DOE Element-specific breach response plans submitted by Secretarial Officers/Heads of Departmental Elements/Heads of Program Offices/Heads of Field Elements.

(10) Conducts annual reviews of Element- and Program Office-specific breach response plans and periodic audits of Element and Program Office breach response activities, if applicable.

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

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

(13) Issues Departmental guidance to Department Elements and Offices 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 when sending PII through electronic means).

(14) Ensures that employees and contractors staffing the iJC3 are properly trained to identify a privacy breach.

(15) Reviews this Appendix 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.

e. Chief Privacy Officer (CPO).

(1) Manages the Department's Privacy Program.

(2) Reviews the Department's PIAs.

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

(4) Coordinates with the CIO; the Chief Health, Safety and Security Officer (AU); GC; and Heads of Departmental Elements to ensure compliance with the requirements of this Order.

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

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

(7) Coordinates with the CISO, senior-level officials in the Office of the CIO, Office of the General Counsel staff, and other stakeholder offices as

appropriate, to assess and investigate reported incidents involving breaches of PII.

(8) 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.

(9) Develop a formal Lessons Learned report following any breach reported to Congress. The SAOP will review the Lessons Learned report with the PIRT to determine whether changes to the Department's Breach Response Plan, policies, training, or other documentation is appropriate, and document specific challenges preventing the Department from instituting appropriate remedial measures.

(10) Supports the iJC3 to develop quarterly reports for the SAOP detailing the status of each breach involving PII reported during the fiscal year.

(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. Monitors implementation of activities reducing the use of SSNs and encouraging the use of encryption when sending PII through electronic means.

(16) Coordinates with the Program Manager for the DOE iJC3 and with the points of contact designated by the Secretarial Officer/Head of DOE Element/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.

f. Chief Information Officer (CIO).

(1) Advises and provides cyber security 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.

g. Privacy Incident Response Team (PIRT).

(1) Convened by the SAOP.

(2) Responds to significant or Major Incidents involving the breach of PII as determined by the SAOP.

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

(4) Coordinates with the SAOP for internal and external agency notification including law enforcement.

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

(6) Is chaired by the SAOP, who may convene the PIRT when the SAOP determines the PII breach:

(a) is a Major Incident;

(b) crosses DOE organizational boundaries; or

(c) is otherwise needed.

(7) Is comprised of the CPO and senior-level officials from the following offices, at a minimum:

(a) the CIO or the CIO's designee;

(b) the CISO;

(c) GC;

(d) CI;

(e) PA; and

(f) the DOE Program Office(s) impacted by a PII breach.

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

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

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

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

h. Privacy Act Officers (PAO) and Privacy Points of Contact (PPOC).

(1) Advocate and promote Privacy program activities within their Departmental Elements.

(2) Advise and provide Privacy Act subject matter expertise to their Departmental Elements, specifically with regard to conducting PIAs and completing the SORN process.

(3) Facilitate compliance reporting for their Departmental Elements or Program Offices.

(4) Assist as needed in privacy breach response.

(5) Manage the process for resolving privacy complaints for their Departmental Elements, including:

(a) documentation of factual circumstances surrounding unresolved complaints and

(b) notifying the CPO of unresolved written complaints.

i. Integrated Joint Cybersecurity Coordination Center (iJC3).

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

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

(3) Notifies CPO and the CISO of all incidents involving the breach of PII *within ONE HOUR* of receiving initial notification.

(4) Reports breaches of PII to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives *within ONE HOUR* of receiving the report of a breach.

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

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

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

j. Senior Procurement Executive, Office of Management.

(1) Ensures that Departmental 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.

k. Contracting Officers.

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

(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 at 52.224-1 and 52.224-2 are included in all solicitations and in any awarded contracts.

(4) If a contracting officer receives a report of a suspected or confirmed breach of PII, the contracting officer will confirm that the report has been submitted to iJC3.

l. DOE Employees.

(1) Are responsible for safeguarding PII in all forms including written, verbal, and electronic. Safeguarding includes encrypting emails or password-protecting attachments with sensitive or High Risk PII before sending, particularly when sending outside of DOE.

(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 B, including facilitating reporting to iJC3 and to minimize potential harm.

(3) Are responsible for complying with the Privacy Act.

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

m. System Owners.

(1) System Owners are Departmental Element officials responsible for monitoring the information systems under their purview to ensure compliance with this Order. System Owners are responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of Privacy information including PII for their information system(s).

(2) System Owners must file a SORN, if applicable, and must complete the entire Federal Register review period before the system will be permitted to operate in the production environment.

(3) System Owners must submit documentation in support of a new or revised SOR or significant alteration to an existing SOR to the CPO. All privacy documentation must be in electronic format and submitted via e-mail to privacy@hq.doe.gov. The CPO, in consultation with General Counsel, will post a SORN in the *Federal Register* providing interested persons the opportunity to comment on the SOR.

(4) System Owners must submit documentation to the CPO in sufficient time for the CPO, in consultation with GC, to review prior to placing a SOR in operation.

(5) For each SOR a System Owner maintains, the System Owner must—

(a) Maintain only personal information considered relevant and necessary for the legally valid purpose for which it is obtained;

(b) Where possible, collect information directly from the individual;

(c) Prepare documentation for the publication of notice in the *Federal Register*, when a SOR is established or revised;

(d) Update SORNs prior to any significant change occurring to a System that affects the privacy information kept in the System;

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

(f) Employ appropriate security controls for the system to protect confidentiality, integrity, and available of records; and

(g) Require persons involved in the design, development, operation, or maintenance of any SOR, or in maintaining any record to sign a Rules of Behavior for each SOR to which they are granted access.

n. General Counsel.

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

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

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

6. REFERENCES.

a. Federal Laws and Regulations.

(1) Privacy Act of 1974, as amended at 5 U.S.C. §552a, P.L. 93-579.

(2) E-Government Act of 2002, P.L. 107-347.

(3) Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq*.

(4) DOE Privacy Act Regulation, 10 CFR Part 1008.

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

(6) DOE Regulations Implementing the FOIA, 10 CFR Part 1004.

b. Office of Management and Budget Circulars and Memoranda.

(1) OMB Circular A-130, Managing Information as a Strategic Resource.

(2) OMB Memorandum (M) 99-05, Privacy and Personal Information in Federal Records.

(3) OMB M-99-18, Privacy Policies on Federal Web Sites.

(4) OMB M-00-13, Privacy Policy and Data Collection on Federal Web Sites.

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

(6) OMB M-05-08, Designation of Senior Officials for Privacy.

(7) OMB M-06-15, Safeguarding Personally Identifiable Information.

(8) OMB M-06-16, Protection of Sensitive Agency Information.

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

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

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

(12) OMB M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements.

c. Department of Energy Directives.

(1) DOE P 205.1, *Departmental Cyber Security Management Policy*, current version.

(2) DOE O 205.1, *Department of Energy Cyber Security Program*, current version.

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

(4) DOE O 221.2, *Cooperation with the Office of Inspector General*, current version.

(5) DOE O 471.3, *Identifying and Protecting Official Use Only Information*, current version.

7. DEFINITIONS.

a. Accuracy. Ensuring, within sufficient tolerance for error, the quality of the record in terms of its use in making a determination.

b. Availability. Ensuring timely and reliable access to and use of information or an information system. For example, a loss of availability is the disruption of access to or use of information or an information system.

c. Breach or Data Breach.[1] An incident involving the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

[1] This definitions of "Incident," "Breach," and "Major Incident" are consistent with the definitions established in OMB M-17-12, and OMB Memorandum 18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 16, 2017 (M-18-02) and may differ from similar

- A person other than an authorized user accesses or potentially accesses PII; or

- An authorized user accesses or potentially accesses PII for other than the authorized purpose.

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

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

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.

The Elements of a Breach are further defined as follows:

- Unauthorized modification is the act or process of changing components of information and/or information systems.

- Unauthorized deletion is the act or process of removing information from an information system.

- 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.

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

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

- loss of control or similar occurrence (e.g., unencrypted email transmission) of sensitive or High Risk DOE employee or contractor PII;

- loss of control or similar occurrence of Department credit card holder information;

- loss of control or similar occurrence of PII collected from or pertaining to members of the public;

---

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.

- loss of control or similar occurrence of system security information (e.g., user name, passwords, security question responses, etc.);
- incorrect delivery of PII to an unauthorized person;
- theft of or compromise of PII; and
- 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.

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

- A laptop or removable storage device containing PII is lost or stolen and information on the device is accessed;
- An employee or contractor's system access credentials are lost or stolen to gain access to files containing PII;
- An unencrypted email containing sensitive or High Risk PII is sent to the wrong person, inside or outside of the Department email network;
- Files or documents with PII, such as medical information, are lost or stolen during shipping, courier transportation, or relocation;
- 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;
- An unauthorized person overhears Departmental employees or contractors discussing the PII of another individual; or
- An IT system that collects, maintains, or disseminates PII is accessed or compromised by an unauthorized person or malicious actor.

d. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

e. 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.

f. 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.

g. Identity Theft. Per section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a), "a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation."

h. Incident.[2] An occurrence that:

- Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

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

i. Information Technology (IT). As defined in the Clinger-Cohen Act, Pub. L. No. 104-106, IT refers to any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

j. Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

k. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

l. Major Incident.[3] A breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized

[2] See footnote 1

[3] See footnote 1

deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII automatically constitutes a "major incident."

While the definition of Major Incident includes a numerical threshold, the Department's Senior Agency Official for Privacy (SAOP) will consider the character of the PII and the circumstances of the breach in making this determination, particularly where sensitive or High Risk 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 or High Risk PII of individuals approaching 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.

m. Major Information System. An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

n. 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—

- involves intelligence activities;
- involves cryptologic activities related to national security;
- involves command and control of military forces;
- involves equipment that is an integral part of a weapon or weapons system;
- 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
- 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.

o. Necessary. A threshold of need for an element of information greater than mere relevance and utility. A Federal agency should maintain in its records only such information about an individual as is relevant and reasonably necessary to ensure fairness to the individual and to accomplish a purpose of the agency that is required by statute or by Executive Order.

p. 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.

The sensitivity of PII increases when combinations of elements increase the ability to identify or target a specific individual. PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual is categorized as **High Risk PII**. Examples of High Risk PII include, Social Security Numbers (SSNs), biometric records (*e.g.*, fingerprints, DNA, etc.), health and medical information, financial information (*e.g.*, credit card numbers, credit reports, bank account numbers, etc.), and security information (e.g., security clearance information).

While all PII must be handled and protected appropriately, High Risk PII must be given greater protection and consideration following a breach because of the increased risk of harm to an individual if it is misused or compromised.

q. Privacy Act Information. Information that is required to be protected under the Privacy Act of 1974.

r. 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.

s. Privacy Impact Assessment (PIA). An analysis of how information is handled to—

- ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and
- examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

t. 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.

u. Relevance. A limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

v. Routine Use. With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

w. System of Records. 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.

x. 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.

y. Timeliness. Sufficiently current to ensure that any determination based on the record will be complete, accurate and fair.

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

BY ORDER OF THE SECRETARY OF ENERGY:

DAN BROUILLETTE
Deputy Secretary

APPENDIX A. PRIVACY IMPACT ASSESSMENTS

Why are DOE organizations required to conduct PIAs?

The E-Government Act of 2002 requires Federal agencies to perform Privacy Impact Assessments (PIAs), an analysis of how information is handled, 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 and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The DOE PIA process helps to ensure privacy protections are considered and implemented throughout the system life cycle.

Step 1 – The Privacy Needs Assessment

System Owners are required to complete the first step of the DOE PIA for all unclassified information systems including contractor systems operated for or on behalf of the agency. This first step of the DOE PIA process is the Privacy Needs Assessment (PNA). The PNA is designed to ensure privacy is addressed for all information systems in an efficient manner by asking four threshold questions:

1. Does the information system collect or maintain information about individuals?

2. Is the information in identifiable form?

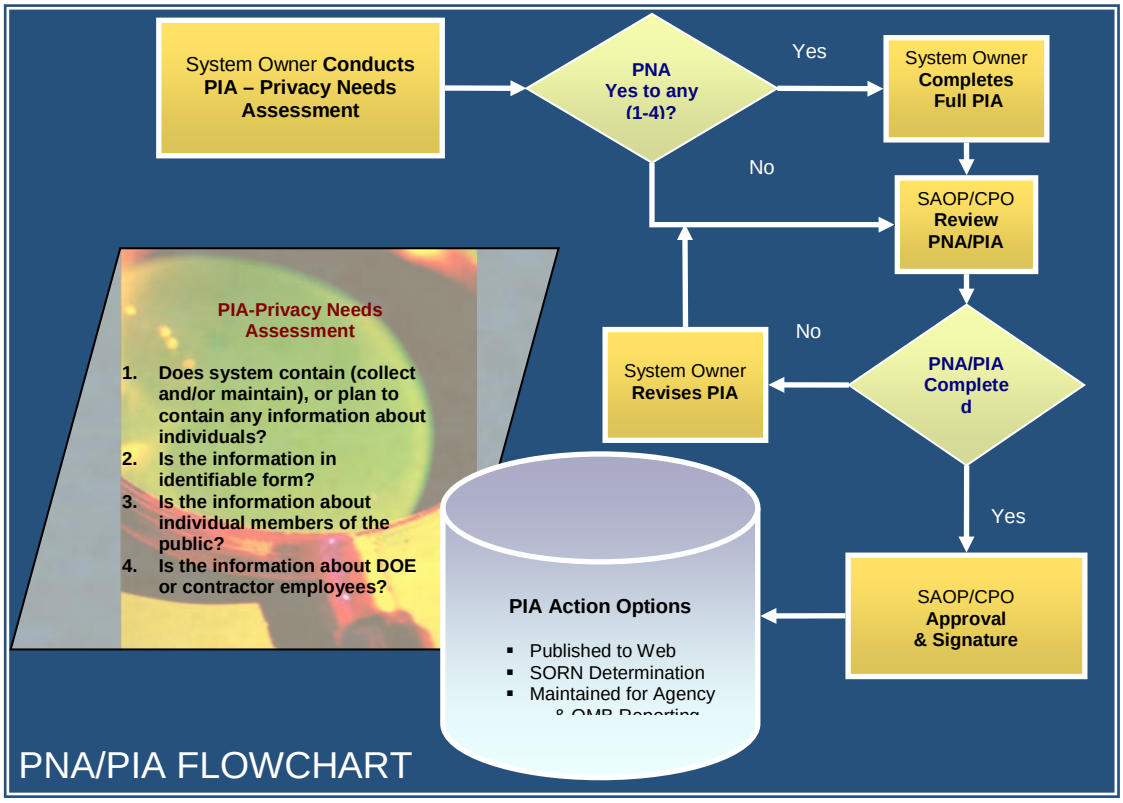
3. Is the information about individual members of the public?

4. Is the information about DOE or contractor employees?

If the answer to any of these questions is "Yes," System Owners must complete a full PIA.

If the answer to <u>all</u> the threshold questions in the PNA is "No," no further sections of the PIA must be completed. The System Owner signs the PIA certifying to the CPO that the system does not contain PII.

System Owners and their Privacy Act Officers must sign the PNA and submit the PNA to the DOE CPO. The PNA/PIA Flowchart illustrates this process.



If the answer to any of the questions in the PNA is "Yes" and a full PIA is required, the System Owner, in collaboration with the Privacy Act Officer must—

- Complete applicable elements of the PIA and
- Sign and submit the PIA to the CPO, copying the Head of the Departmental Element (HDE) staff.

If there are issues with the submitted PIA that need to be addressed, the CPO will coordinate with the System Owner to ensure there is an understanding of any deficiencies in the PIA so corrective action may be taken. The SAOP approves and signs the PIA. The CPO provides a signed copy of the PIA to the System Owner. PIAs affecting members of the public will be posted to the DOE Privacy Website in accordance with applicable laws and regulations. The System Owner may also be required to publish a System of Records Notice in the Federal Register.

When to Conduct a Privacy Impact Assessment

Privacy, like security, should be considered at all stages of the system's lifecycle. Departmental Elements must also consider the information lifecycle (i.e. collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect an individual's privacy. PIAs should be conducted as part of the certification and accreditation process. At a minimum, PIAs must be conducted when—

- Designing, developing or procuring information systems or IT projects that collect, maintain or disseminate information in identifiable form.

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

- Significantly modifying an information system.

PIAs should be updated whenever there is a change to the information system that affects privacy or creates new risks to privacy. Examples of these changes include the following:

- **Conversions** - when converting paper-based records to electronic systems.

- **Anonymous to Non-Anonymous** - when functions applied to an existing information collection change anonymous information into information in identifiable form.

- **Significant System Management Changes** - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.

- **Significant Merging** - when organizations adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.

- **New Public Access** - when authentication technology (e.g., password, digital certificate, biometric) is newly applied to an information system accessed by members of the public.

- **Commercial Sources** - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources (merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement).

- **New Interagency Uses** - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA.

- **Internal Flow or Collection** - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.

- **Alteration in Character of Data** - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

- **Changed Authorities or Business Processes** - when there are changes in information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

Who Completes the Privacy Impact Assessment?

The PIA is the System Owner's responsibility. The System Owner, system developer, data owners and the Privacy Act Officer must work together to complete the PIA.

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

Privacy Impact Assessment Document Review and Approval Process

The completed PIAs must be submitted to the CPO, copying the Heads of Departmental Elements' staff. The CPO submits the PIAs to the SAOP for approval and signature.

If the Chief Privacy Officer indicates corrective action is necessary for a PIA, the PIA will be returned to the System Owner. The System Owner is responsible for identifying and implementing corrective actions prior to resubmitting the PIA to the CPO.

Steps for Completing the DOE Privacy Impact Assessment

Step	Responsible Individual(s)	Actions
1	**System Owner**	**PIA Template** Obtain current DOE PIA template from the Privacy Website. The System Owner has the overall responsibility and accountability for completing the PIA. Privacy should be considered at all stages of the system lifecycle. At a minimum, the PIA should be conducted as part of the certification and accreditation of the system and reviewed at least annually.
2	**System Owner** **Privacy Act Officer**	**Complete PNA portion of the PIA** A. If the answer to <u>all</u> questions on the PNA section of the PIA is "No," the System Owner and Privacy Act Officer must sign and submit the PNA to the CPO, copying the HDE staff. Upon receiving the approval of the SAOP, the PIA is now complete. B. If the answer to <u>any</u> of the questions on PNA is "Yes," proceed to step 3.
3	**System Owner** ▪ Privacy Act Officer ▪ System Administrators ▪ Data Owners ▪ Program Managers ▪ Subject Matter Experts ▪ Information System Security Officer ▪ Security: Cyber & Physical Security ▪ Operations	**Conduct Full PIA** Complete full PIA using DOE PIA template. The template is available from the Privacy Website, and may not be modified. System Owners and Privacy Act Officers must Sign the PIA.
4	**System Owner** **DOE CPO** **DOE CIO**	**Submit PIA to CPO** System Owner submits PIA to CPO for review. The CPO may consult with subject matter experts and GC. If there are any issues with the PIA, the CPO will coordinate with the System Owner to ensure deficiencies are identified. The System Owner corrects deficiencies and resubmits the PIA. Depending on the scope and number of deficiencies, the System Owner may develop a plan of action and milestones for correcting the PIA. Once all deficiencies and concerns have been addressed, the System Owner resubmits the PIA to the DOE CPO.
5	**DOE CPO** **SAOP**	**DOE CPO Submits to SAOP** Having reviewed the PIA, the CPO submits the PIA to the SAOP for signature.
6	**SAOP** **DOE CPO**	**SAOP Signature and Approval**

Step	Responsible Individual(s)	Actions
	System Owner	The SAOP approves and signs the PIA. Copies of the signed PIA are maintained with the CPO and provided to the System Owner for their records. The System Owner should maintain these records for conducting certification and accreditation and for preparing OMB Exhibits 300 and 53.
7	**SAOP** **CPO** **General Counsel** **System Owner** **Privacy Act Officer**	**System Requires Web Posting and Reporting** If the PIA identifies the system as a system affecting members of the public in accordance with the E-Government Act, the following actions are taken: ▪ CPO posts the signed PIA affecting members of the public to the DOE Privacy website; ▪ Publishes System of Records Notice in the Federal Register, if applicable; ▪ Reports PIAs affecting members of the public to OMB. NOTE: Not all PIAs require a SORN; therefore, there will not be a one-to-one (1:1) ratio of PIAs to SORNs.
8	**System Owner** **Privacy Act Officer**	**Ongoing Monitoring** The System Owner and local Privacy Act Officer will ensure the PIA is reviewed at least annually or whenever there is a change to the system that would impact the risk to privacy. If required, the PIA is updated.

Department of Energy
Privacy Impact Assessment Privacy Needs Assessment

<SAMPLE ONLY>		
Date		
Departmental Element		
Name of Information System or IT Project		
Exhibit Project UID		
	Name, Title	Contact Information Phone, Email
System Owner		
Privacy Act Officer		
Purpose of Information System or IT Project		
Type of Information Contained (Collected or Maintained) Use NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance.		
Has there been any attempt to verify Information in Identifiable Form does not exist on the system (e.g., system scan)?		
If "Yes," what method was used to verify the system did not contain Information in Identifiable Form?		

Threshold Questions	
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	
2. Is the information in identifiable form?	
3. Is the information about individual members of the public?	
4. Is the information about DOE or contractor employees?	
If the answer to the **all** four (4) key threshold questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.	

APPENDIX B. 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, in external locations (e.g., when an employee or contractor is on official travel, and in cloud service environments).

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

(a) to the local PAO and/or PPOC AND the Integrated Joint Cybersecurity Command Center (iJC3) at 866-941-2472 (or via email to circ@jc3.doe.gov); OR

(b) through their Departmental Element in accordance with existing cyber incident reporting processes, which have been established in Senior DOE Management Program Cyber Security Plans (PCSPs) as defined in DOE O 205.1, *Department of Energy Cyber Security Program*, current version.

(3) Reports should include:

(a) the date and time of discovery of the breach;

(b) the type(s) of PII involved;

(c) number of impacted individuals;

(d) whether the impacted individuals are members of the public;

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

(f) whether the information was encrypted or secured at the time of the breach; and

(g) 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 US-CERT.

(a) The iJC3 will ensure that the CPO and the CISO are notified of all breaches of PII within ONE HOUR of receiving notification.

(b) 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.

(c) 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 Privacy Program 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 that reduce the risk to PII were, 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.

(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 IG 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; (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 identify 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 or Congressional committees in advance of the Department providing formal notice.

(4) The Department will seek to provide notification to 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 Departmental Element/Head of Program Office, or their authorized designee.

(a) Preliminary notice will be provided in accordance to 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 or password protection, 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 the (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.

(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 or High Risk PII, such as SSNs, financial information, or health information, which has been sent unsecure via email (*i.e.*, unencrypted or without password protection) 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 or High Risk 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 E-government.

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 the Appendix (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 have 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.

(3) Completion of Mandatory Annual Privacy Training.

(a) All DOE employees with access to DOE Enterprise IT networks must complete mandatory Privacy Awareness training.

(b) Employees with job-responsibilities involving the collection, storage, maintenance, and sharing of PII in either physical or electronic formats are subject to additional privacy training, appropriate to the nature of their job functions.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 206.1, *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 design, development or operation of a Privacy Act System of Record. In addition, the Personally Identifiable Information (PII) requirements in this CRD apply to any site management contractor that handles PII. This CRD applies to Federal information held by a contractor created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is 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.

1. GENERAL REQUIREMENTS.

   a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, and take appropriate actions to assist DOE in complying with Section 208 of the E-Government Act of 2002, and associated Office of Management and Budget (OMB) directives.

   b. Ensure that contractor employees are aware of their responsibility for—

      (1) safeguarding Personally Identifiable Information (PII);

      (2) reporting suspected or confirmed breach of PII; and

      (3) complying with the Privacy Act, when required.

2. SPECIFIC REQUIREMENTS. The contractor must do the following:

   a. Ensure contractor employees are made aware of their roles and responsibilities for reporting suspected or confirmed breach of PII.

   b. Ensure contractor employees are cognizant of the following DOE Privacy Rules of Conduct. At a minimum, ensure contractor employees:

      (1) Are trained in their responsibilities regarding the safeguarding of PII.

      (2) Do not disclose any PII contained in any SOR except as authorized.

      (3) Report any suspected or confirmed breach of PII involving Federal information, without unreasonable delay, consistent with the agency's breach response procedures outlined in DOE O 206.1 and US-CERT notification guidelines.

(4) Assist with the investigation and mitigation of harm (including necessary PII removal or encryption within the IT system, notifications, credit monitoring, and other appropriate measures) following a breach of PII involving Federal information under the custody of the contractor.

(5) Observe the requirements of DOE directives concerning marking and safeguarding sensitive information, including, when applicable, DOE O 471.3, *Identifying and Protecting Official Use Only Information*, current version.

(6) Collect only the minimum PII necessary for the proper performance of a documented agency function.

(7) Do not place PII on shared drives, intranets or websites without permission of the System Owner.

(8) Challenge anyone who asks to see the PII for which they are responsible.

c. Ensure that contractor employees complete an Annual Privacy Awareness Training that includes the requirements of DOE O 206.1 and sign the completion certificate acknowledging their responsibility for maintaining and protecting Privacy Act information prior to being authorized access to all information systems.

d. Ensure contractor employees are cognizant of the fact that PII subject to the requirements of the Privacy Act must be maintained in a Privacy Act SOR.

e. Ensure that contractor employees recognize differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, contractors must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act. PII not maintained in a Privacy Act SOR should be protected and only disclosed for authorized purposes.

f. Ensure contractor employees are cognizant of the fact that non-compliance with the Privacy Act carries criminal and civil penalties.

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