

**U.S. Department of Energy**  
**Washington, DC**

**MINOR CHANGE**

**DOE O 206.1**

Chg 1 (Min Chg): 11-1-2018

**SUBJECT: MINOR CHANGES TO DOE O 206.1, *DEPARTMENT OF ENERGY PRIVACY PROGRAM***

---

1. EXPLANATION OF CHANGES. This update formalizes the Department's privacy breach response plan. Changes were also made to update references to other DOE directives.
2. LOCATIONS OF CHANGES:

Page	Paragraph	Changed	To
1	1.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 Office of Management and Budget (OMB) directives.	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.
1	2	<u>CANCELLATION.</u> DOE N 206.5, Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information, dated 10-09-07, is canceled.	<u>CANCELS/SUPERSEDES.</u> DOE O 206.1, Department of Energy Privacy Program, dated 01-16-09, is canceled.
1	3.a.	<u>DOE Elements.</u> Except for the exclusions in paragraph 3.c., this Order applies to all Departmental Elements, including those created after the Order is issued. (Go to <a href="http://www.directives.doe.gov/pdfs/reftools/org-list.pdf">www.directives.doe.gov/pdfs/reftools/org-list.pdf</a> for the current listing of Departmental Elements.)	<u>DOE Elements.</u> Except for the exclusions in paragraph 3.c., this Order applies to all Departmental Elements, including those created after the Order is issued.
2	3.c.(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	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

Page	Paragraph	Changed	To
		practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.	oversee requirements and practices pertaining to this Order for activities under the Director's cognizance, as deemed appropriate.
2	3.c.(2)	Added.	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.
2	4.a.(3)	Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees must immediately report the incident to the DOE-Cyber Incident Response Capability (DOE-CIRC) at 866-941-2472 ( <a href="mailto:doecirc@doecirc.energy.gov">doecirc@doecirc.energy.gov</a> ) and 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 205.1A, Department of Energy Cyber Security Management.	<p>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:</p> <p>(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 (<u>or via email to <a href="mailto:circ@jc3.doe.gov">circ@jc3.doe.gov</a></u>); OR</p> <p>(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,</p>

Page	Paragraph	Changed	To
			Department of Energy Cyber Security Program, current version.
2	4.a.(4)-(5)	<p>(4) Types of breaches that must be reported include, but are not limited to the following:</p> <ul style="list-style-type: none"> <li>(a) loss of control of DOE employee information consisting of names and Social Security numbers,</li> <li>(b) loss of control of Department credit card holder information,</li> <li>(c) loss of control of PII pertaining to the public,</li> <li>(d) loss of control of security information (e.g., logons, passwords, etc.),</li> <li>(e) incorrect delivery of PII,</li> <li>(g) theft of PII, and</li> <li>(g) unauthorized access to PII stored on Department-operated web sites.</li> </ul> <p>(5) Within one hour of receiving the report of an incident involving a breach of PII, the Office of the Chief Information Officer (OCIO) will report the incident to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives. The OCIO will ensure the Chief Privacy Officer (CPO) is notified of all incidents involving the breach of PII within one hour of receiving notification.</p>	Removed.
3	4.a.(6)-(7)	Renumbered	4.a.(4)-(5)

Page	Paragraph	Changed	To
5	4.b.(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 and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.	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.
5	4.b.(15)	Senior DOE Management, as defined in DOE O 205.1A, Department of Energy Cyber Security Management, dated 12-4-06, 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.	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	5.a.-k.	<p>Added and Reorganized.</p> <ul style="list-style-type: none"> <li>a. Senior Agency Official for Privacy</li> <li>b. Director, Office of Information Resources</li> <li>c. Chief Privacy Officer</li> <li>d. Secretarial Officers/Heads of Departmental Elements</li> <li>e. Chief Information Officer</li> <li>f. Privacy Incident Response Team (PIRT)</li> <li>g. Privacy Act Officers</li> <li>h. Contracting Officers</li> <li>i. DOE Employees</li> <li>j. System Owners</li> </ul>	<p>5.a.-n.</p> <ul style="list-style-type: none"> <li>a. Secretary of Energy (S1).</li> <li>b. Deputy Secretary of Energy (S2)</li> <li>c. Secretarial Officers/Heads of Departmental Elements/Heads of Program Offices/Heads of Field Offices</li> <li>d. Senior Agency Official for Privacy (SAOP)</li> <li>e. Chief Privacy Officer (CPO)</li> <li>f. Chief Information Officer (CIO)</li> <li>g. Privacy Incident Response Team (PIRT)</li> </ul>

Page	Paragraph	Changed	To
		k. General Counsel	<ul style="list-style-type: none"> <li>h. Privacy Act Officers (PAO) and Privacy Point of Contact (PPOC)</li> <li>i. Integrated Joint Cybersecurity Coordination Center (iJC3)</li> <li>j. Senior Procurement Executive, Office of Management</li> <li>k. Contracting Officers</li> <li>l. DOE Employees</li> <li>m. System Owners</li> <li>n. General Counsel</li> </ul>
5	5.a.		<p>New 5.a.</p> <p><u>Secretary of Energy (S1).</u></p> <ul style="list-style-type: none"> <li>(1) Designates the Department's SAOP.</li> <li>(2) Designates the standing group of Departmental representatives to the Privacy Incident Response Team (PIRT), which will include, at a minimum: <ul style="list-style-type: none"> <li>(a) The Department's SAOP;</li> <li>(b) the Department's Chief Privacy Officer (CPO);</li> <li>(c) the Chief Information Officer (CIO) or the CIO's designee;</li> <li>(d) the Chief Information Security Officer (CISO);</li> <li>(e) a senior official from the Office of the General Counsel (GC);</li> <li>(f) the Office of Congressional and Intergovernmental Affairs (CI); and</li> <li>(g) the Office of Public Affairs (PA).</li> </ul> </li> </ul>

Page	Paragraph	Changed	To
			<p>The SAOP may invite other Department officials and subject matter experts as necessary to serve on the PIRT.</p> <p>(3) Makes a final decision on whether the Department will provide notification.</p> <p>(4) Makes a determination on whether additional identity protection services will be provided to individuals affected by a breach involving PII.</p> <p>(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.</p> <p>(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.</p>
5	5.b.	Added.	<p>New 5.b.</p> <p><u>Deputy Secretary of Energy (S2).</u></p> <p>(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.</p> <p>(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.</p>

Page	Paragraph	Changed	To
6	5.c.	Was 5.d. Secretarial Officers/Heads of Departmental Elements	Renumbered to 5.c. Secretarial Officers/Heads of Departmental Elements/Heads of Program Offices/Heads of Field Offices
7	5.c.(7)-(12)	Added.	<p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(11) Ensure that breaches involving PII in any form—written, electronic, or verbal—are</p>

Page	Paragraph	Changed	To
			<p>reported to both the Department's Integrated Joint Cybersecurity Coordination Center (iJC3) and the SAOP IMMEDIATELY.</p> <p>(12) Ensure responsibility for all costs associated with remediation including notification of affected or potentially-affected individuals for breaches originating within their Element.</p>
8	5.d.(2)-(15)	<p>Was 5.a.</p> <p>Added.</p>	<p>Renumbered to 5.d.</p> <p>(2) Oversees Departmental response to breaches involving PII.</p> <p>(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.</p> <p>(4) Determines whether a breach meets the criteria of a Major Incident.</p> <p>(5) Determines whether a breach of PII reported by an Element or Program Office should be handled by Headquarters staff, based on:</p> <ul style="list-style-type: none"> <li>(a) the scope and impact of the breach, including the number of affected persons;</li> <li>(b) whether the breach involves at least two or more DOE Elements or Offices; or</li> <li>(c) the SAOP's determination that it is otherwise significant.</li> </ul> <p>(6) Convenes and chairs the PIRT. The PIRT shall always be convened when a breach constitutes a Major Incident.</p> <p>(7) Develops and conducts tabletop exercises for PIRT</p>



Page	Paragraph	Changed	To
			<p>members, at least annually, and provides additional training as appropriate.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(12) Reports metrics on breaches involving PII impacting the Department under quarterly and annual Federal Information Security Modernization Act (FISMA) reporting requirements.</p> <p>(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).</p>

Page	Paragraph	Changed	To
			<p>(14) Ensures that employees and contractors staffing the iJC3 are properly trained to identify a privacy breach.</p> <p>(15) Reviews this Appendix annually and considers whether DOE should:</p> <ul style="list-style-type: none"> <li>(a) Update its breach response plan;</li> <li>(b) Develop and implement new policies to protect the agency's PII holdings;</li> <li>(c) Revise existing policies to protect the agency's PII holdings;</li> <li>(d) Reinforce or improve training and awareness;</li> <li>(e) Modify information sharing arrangements; and</li> <li>(f) Develop or revise documentation such as System of Record Notices (SORNs), PIAs, or privacy policies.</li> </ul>
9	5.e.(5)-(16)	Was 5.c. Added.	<p>Renumbered to 5.e.</p> <p>(5) Manages implementation of the Department's breach response process and supports the SAOP.</p> <p>(6) Serves as the SAOP's authorized designee for privacy incident response, as needed.</p> <p>(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.</p> <p>(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</p>

Page	Paragraph	Changed	To
			<p>actions taken to mitigate potential harms or prevent similar future occurrences.</p> <p>(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.</p> <p>(10) Supports the iJC3 to develop quarterly reports for the SAOP detailing the status of each breach involving PII reported during the fiscal year.</p> <p>(11) Serves as the Subject Matter Expert (SME) on policy, legislation, regulations, and guidance related to information privacy.</p> <p>(12) Maintains an inventory of Departmental systems containing PII on behalf of the SAOP.</p> <p>(13) Ensures that Privacy Act SORNs are kept current.</p> <p>(14) Uses Departmental PIAs and SORNs as resources in privacy incident response or breach investigations</p> <p>(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</p> <p>(16) Coordinates with the Program Manager for the DOE iJC3 and with the points of contact</p>

Page	Paragraph	Changed	To
			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.
11	5.f.	<p>Was 5.e.</p> <p>Chief Information Officer.</p> <p>(1) Advises and provides cyber security and information technology subject matter expertise to the CPO to identify ways in which the Department can safeguard privacy information.</p> <p>(2) Provides current threat information regarding the compromise of PII and information systems containing PII.</p> <p>(3) Reports incidents involving breaches of PII to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives and ensures the CPO is notified of all incidents involving the breach of PII within one hour of receiving notification</p>	<p>Renumbered to 5.f.</p> <p>Chief Information Officer (CIO).</p> <p>(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.</p> <p>(2) Provides current threat information regarding the compromise of PII and information systems containing PII.</p> <p>(3) Ensures the SAOP and the CPO are notified of all breaches of PII within ONE HOUR of receiving notification.</p>
11	5.g.	<p>Was 5.f.</p> <p>Privacy Incident Response Team (PIRT).</p> <p>(1) Convened by the SAOP.</p> <p>(2) Responds to major incidents involving the breach of PII as determined by the SAOP.</p> <p>(3) Conducts assessments of incidents involving breaches of privacy data, including evaluating the scope, degree of compromise, impact and risks resulting from the breach.</p>	<p>Renumbered to 5.g.</p> <p>Privacy Incident Response Team (PIRT).</p> <p>(1) Convened by the SAOP.</p> <p>(2) Responds to significant or Major Incidents involving the breach of PII as determined by the SAOP.</p> <p>(3) Conducts assessments of the breach of PII, including evaluating the scope, degree of compromise, impact and risks resulting from the breach.</p>

Page	Paragraph	Changed	To
		(4) Coordinates with the SAOP for internal and external agency notification including law enforcement.	(4) Coordinates with the SAOP for internal and external agency notification including law enforcement.
11	5.g.(5)-(10)	Added.	<p>(5) Serves as the Breach Response Team required by OMB M-17-12.</p> <p>(6) Is chaired by the SAOP, who may convene the PIRT when the SAOP determines the PII breach:</p> <ul style="list-style-type: none"> <li>(a) is a Major Incident;</li> <li>(b) crosses DOE organizational boundaries; or</li> <li>(c) is otherwise needed.</li> </ul> <p>(7) Is comprised of the CPO and senior-level officials from the following offices, at a minimum:</p> <ul style="list-style-type: none"> <li>(a) the CIO or the CIO's designee;</li> <li>(b) the CISO;</li> <li>(c) GC;</li> <li>(d) CI;</li> <li>(e) PA; and</li> <li>(f) the DOE Program Office(s) impacted by a PII breach.</li> </ul> <p>The SAOP may invite other Department officials and subject matter experts as necessary to serve on the PIRT.</p> <p>(8) Adds specialized members, including, but not limited to, budget and procurement personnel, human resource personnel, and/or physical security personnel, as circumstances warrant.</p> <p>(9) Coordinates with the IG to ensure significant PII</p>

Page	Paragraph	Changed	To
			<p>breaches involving alleged or suspected crimes are reviewed for potential IG investigation.</p> <p>(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.</p>
11	5.h.	Was 5.g. Privacy Act Officers	Renumbered to 5.h. Privacy Act Officers (PAO) and Privacy Points of Contact (PPOC)
11	5.h.(3)	Facilitate compliance reporting for their Departmental Elements.	Facilitate compliance reporting for their Departmental Elements or Program Offices.
11	5.h.(4)	Added	Assist as needed in privacy breach response.
11	5.h.(4)	Renumbered	5.h.(5)
12	5.i.	Added.	<p>New 5.i.</p> <p>Integrated Joint Cybersecurity Coordination Center (iJC3).</p> <p>(1) Serves as the Department's Security Operations Center (SOC) for cyber incidents and privacy breaches involving Departmental headquarters IT systems.</p> <p>(2) Receives reports of suspected or confirmed breaches of PII, regardless of format.</p> <p>(3) Notifies CPO and the CISO of all incidents involving the breach of PII within ONE HOUR of receiving initial notification.</p> <p>(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.</p>

Page	Paragraph	Changed	To
			<p>(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.</p> <p>(6) Tracks metrics for all Departmental incidents and breaches for FISMA reporting.</p> <p>(7) Provides quarterly reports to the SAOP detailing the status of each breach reported to the iJC3 during the fiscal year.</p>
13	5.j.	Added.	<p>New 5.j.</p> <p>Senior Procurement Executive, Office of Management.</p> <p>(1) Ensures that Departmental contracts include requirements regarding contractor compliance with Department or DOE Element-approved breach response plans.</p> <p>(2) Works with SAOP to address deficiencies in contractor compliance with applicable privacy laws and compliance requirements.</p>
13	5.k.(2)	<p>Was 5.h.</p> <p>Ensure that contracting officers' representatives (CORs) and/or contracting officers' technical representatives (COTRs) are aware of provisions within this Order and any changes to their respective contracts</p>	<p>Renumbered to 5.k.</p> <p>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</p>
13	5.k.(4)	Added.	<p>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.</p>
13	5.l.	Was 5.i.	<p>Renumbered to 5.l.</p> <p>DOE Employees.</p>

Page	Paragraph	Changed	To
		<p>DOE Employees. Are responsible for safeguarding PII and for reporting suspected or confirmed incidents involving the breach of PII, in printed or electronic form, in accordance with the requirements provided in Appendix B.</p> <p>(2) Are responsible for complying with the Privacy Act.</p>	<p>(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.</p> <p>(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.</p> <p>(3) Are responsible for complying with the Privacy Act.</p> <p>(4) Cooperate with incident response teams that are investigating or attempting to resolve breaches of PII.</p>
15	5.n.	<p>Was 5.k.</p> <p>Added (3).</p>	<p>Renumbered to 5.n.</p> <p>Serves as lead on matters of law and the interpretations of law and regulations pertaining to privacy breach response.</p>
15	6.b.(1)	OMB Circular A-130, Management of Federal Information Resources.	OMB Circular A-130, Managing Information as a Strategic Resource.
15	6.b.(10)	Added.	OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy.
15	6.b.(11)	<p>Was 6.b.(10).</p> <p>OMB M-07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information.</p>	<p>Renumbered to 6.b.(11)</p> <p>OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.</p>



Page	Paragraph	Changed	To
15	6.b.(12)	Added.	OMB M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements.
16	6.c.	<p>Department of Energy Directives.</p> <p>(1) DOE P 205.1, Departmental Cyber Security Management Policy, dated 5-8-01.</p> <p>(2) DOE O 205.1A, Department of Energy Cyber Security Management, dated 12-4-06.</p> <p>(3) DOE N 221.14, Reporting Fraud, Waste, and Abuse, dated 12-20-07.</p> <p>(4) DOE O 221.1A, Reporting Fraud, Waste, and Abuse to the Office of Inspector General, dated 4-19-08.</p> <p>(5) DOE O 221.2A, Cooperation with the Office of Inspector General, dated 2-25-08.</p>	<p>Department of Energy Directives.</p> <p>(1) DOE P 205.1, Departmental Cyber Security Management Policy, current version.</p> <p>(2) DOE O 205.1, Department of Energy Cyber Security Program, current version.</p> <p>(3) DOE O 221.1, Reporting Fraud, Waste and Abuse to the Office of Inspector General, current version.</p> <p>(4) DOE O 221.2, Cooperation with the Office of Inspector General, current version.</p> <p>(5) DOE O 471.3, Identifying and Protecting Official Use Only Information, current version.</p>
17	7.c.	<p><u>Breach</u>. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users—and for other than an authorized purpose—have access to or potential access to PII, whether in physical or electronic form.</p>	<p><u>Breach or Data Breach</u>.<sup>1</sup> An incident involving the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:</p> <ul style="list-style-type: none"> <li>• A person other than an authorized user accesses or potentially accesses PII; or</li> <li>• An authorized user accesses or potentially accesses PII for other than the authorized purpose.</li> </ul> <p>Breaches do not require evidence of harm to an individual, or of unauthorized modification, deletion, exfiltration, or access to information.</p>

<sup>1</sup> 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 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.

Page	Paragraph	Changed	To
			<p>PII can be breached in any format, including physical (paper), electronic, and verbal/oral.</p> <p>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.</p> <p>The Elements of a Breach are further defined as follows:</p> <ul style="list-style-type: none"> <li>• Unauthorized modification is the act or process of changing components of information and/or information systems.</li> <li>• Unauthorized deletion is the act or process of removing information from an information system.</li> <li>• 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.</li> <li>• Unauthorized access is the act or process of logical or physical access without permission to a Federal agency information system, application, or other resource.</li> </ul> <p>Examples of breaches that must be reported include, but are not limited to the following:</p> <ul style="list-style-type: none"> <li>• loss of control or similar occurrence (e.g., unencrypted email transmission) of sensitive or High Risk DOE employee or contractor PII;</li> <li>• loss of control or similar occurrence of Department credit card holder information;</li> </ul>

Page	Paragraph	Changed	To
			<ul style="list-style-type: none"> <li>• loss of control or similar occurrence of PII collected from or pertaining to members of the public;</li> <li>• loss of control or similar occurrence of system security information (e.g., user name, passwords, security question responses, etc.);</li> <li>• incorrect delivery of PII to an unauthorized person;</li> <li>• theft of or compromise of PII; and</li> <li>• unauthorized access to PII stored on Department-managed information systems or managed for the Department, including websites, data centers, cloud services, etc.</li> </ul> <p>For these purposes, reportable PII does not include common business exchanges such as names and/or business contact information.</p> <p>Examples of breaches of PII include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• A laptop or removable storage device containing PII is lost or stolen and information on the device is accessed;</li> <li>• An employee or contractor's system access credentials are lost or stolen to gain access to files containing PII;</li> <li>• An unencrypted email containing sensitive or High Risk PII is sent to the wrong person, inside or outside of the Department email network;</li> <li>• Files or documents with PII, such as medical information, are lost or stolen during shipping, courier transportation, or relocation;</li> </ul>

Page	Paragraph	Changed	To
			<ul style="list-style-type: none"> <li>• 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;</li> <li>• An unauthorized person overhears Departmental employees or contractors discussing the PII of another individual; or</li> <li>• An IT system that collects, maintains, or disseminates PII is accessed or compromised by an unauthorized person or malicious actor.</li> </ul>
19	7.e.	Data Breach Analysis (for incidents involving the breach of PII). The process of assessing what, if any, Privacy information was compromised, the significance of such losses or intrusions, and how to prevent future occurrences.	Removed.
19	7.e.-f.	Added.	<p>e. <u>Federal Information</u>. Information that is created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.</p> <p>f. <u>Federal Information system</u>. 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.</p>
19	7.f.	Renumbered.	7.g.
19	7.h.	Added.	<p><u>Incident</u>.<sup>2</sup> An occurrence that:</p> <ul style="list-style-type: none"> <li>• Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of</li> </ul>

<sup>2</sup> See footnote 1

Page	Paragraph	Changed	To
			<p>information or an information system; or</p> <ul style="list-style-type: none"> <li>• Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.</li> </ul> <p>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</p>
19	7.g.	Information in Identifiable Form. Information in an IT system or online collection: (1) that directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, email address, etc.) or (2) by which an agency intends to identify specific individuals in conjunction with other data elements (i.e. indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors.	Removed.
19	7.h.-j.	Renumbered.	7.i.-k.
20	7.l.	Added.	<u>Major Incident</u> . <sup>3</sup> 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 deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more

<sup>3</sup> See footnote 1

Page	Paragraph	Changed	To
			<p>individuals' PII automatically constitutes a "major incident."</p> <p>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.</p>
20	7.k.-m.	Renumbered.	7.m.-o.
21	7.p.	<p>Was 7.n.</p> <p><u>Personally Identifiable Information (PII)</u>. 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.</p>	<p>Renumbered to 7.p.</p> <p><u>Personally Identifiable Information (PII)</u>. 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.</p> <p>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</p>

Page	Paragraph	Changed	To
			<p>categorized as <b>High Risk PII</b>. 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).</p> <p>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.</p>
24	8	<u>NECESSITY FINDING STATEMENT</u> . In compliance with Sec. 3174 of P.L. 104-201 (50 U.S.C. 2584 note), DOE hereby finds that this Order is necessary for the fulfillment of current legal requirements and conduct of critical administrative functions.	Removed.
	Appendix B	Reorganized to match DOE Order template.	
App B B-1	Title and Introduction	<p><b>APPENDIX B. RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION</b></p> <p>The purpose of this appendix is to define notification requirements and procedures for incidents involving breaches of PII.</p>	<p><b>APPENDIX B. RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION</b></p> <p>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</p>

Page	Paragraph	Changed	To
			Personally Identifiable Information, dated January 3, 2017 (M-17-12) and other subsequent governance related to cybersecurity and privacy incident response.
App B B-1	1.a.(1)	Added.	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).
App B B-1	1.a.(2)-(3)	<p>Was 1.-2.</p> <ol style="list-style-type: none"> <li>1. Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees will immediately report the incident to the DOE-Cyber Incident Response Capability (DOE-CIRC) at 866-941-2472 (<a href="mailto:doecirc@doecirc.energy.gov">doecirc@doecirc.energy.gov</a>) and 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 to DOE O 205.1A, Department of Energy Cyber Security Management.</li> <li>2. Types of breaches that must be reported include, but are not limited to the following: <ol style="list-style-type: none"> <li>a. loss of control of DOE employee information consisting of names and Social Security numbers;</li> <li>b. loss of control of Department credit card holder information;</li> <li>c. loss of control of PII pertaining to the public;</li> </ol> </li> </ol>	<p>Renumbered to 1.a.(2)-(3).</p> <ol style="list-style-type: none"> <li>(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: <ol style="list-style-type: none"> <li>(a) to the local PAO and/or PPOC AND the Integrated Joint Cybersecurity Command Center (iJC3) at 866-941-2472 (<u>or via email to <a href="mailto:circ@jc3.doe.gov">circ@jc3.doe.gov</a></u>); OR</li> <li>(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.</li> </ol> </li> <li>(3) Reports should include: <ol style="list-style-type: none"> <li>(a) the date and time of discovery of the breach;</li> <li>(b) the type(s) of PII involved;</li> </ol> </li> </ol>



Page	Paragraph	Changed	To
		<ul style="list-style-type: none"> <li>d. loss of control of security information (e.g., logons, passwords, etc.);</li> <li>e. incorrect delivery of sensitive PII;</li> <li>f. theft of PII; and</li> <li>g. unauthorized access to PII stored on Department operated web sites.</li> </ul>	<ul style="list-style-type: none"> <li>(c) number of impacted individuals;</li> <li>(d) whether the impacted individuals are members of the public;</li> <li>(e) the location of the PII (physical location, if it is spoken in conversation, or if an IT system involved);</li> <li>(f) whether the information was encrypted or secured at the time of the breach; and</li> <li>(g) a point of contact for follow-up questions or information gathering.</li> </ul>
App B B-2	1.a.(4)	Added.	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.
App B B-2	1.a.(5)	<p>Was 3.</p> <p>Within one hour of receiving the report of an incident involving a breach of PII, the Office of the Chief Information Officer (OCIO) will report the incident to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives. The OCIO will ensure the CPO is notified of all incidents involving the breach of PII within one hour of receiving notification</p>	<p>Renumbered to 1.a.(5).</p> <p>Within ONE HOUR of receiving the report of a breach of PII, the iJC3 will report the breach to the US-CERT.</p> <ul style="list-style-type: none"> <li>(a) The iJC3 will ensure that the CPO and the CISO are notified of all breaches of PII within ONE HOUR of receiving notification.</li> <li>(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.</li> <li>(c) The SAOP and CIO, for cyber-related breaches of PII, may request assistance from senior-level officials and subject matter experts with</li> </ul>

Page	Paragraph	Changed	To
			appropriate technical and risk assessment expertise to assist the CPO's team with the initial assessment.
App B B-2	1.b.-c.	<p>Was 4.-7.</p> <p>4. Additionally, the Senior Agency Official for Privacy may convene the Privacy Incident Response Team (PIRT) chaired by the Senior Agency Official for Privacy, and comprised of senior-level representatives from the Offices of the Chief Information Officer; Public Affairs; General Counsel; Office of Management; Office of Health, Safety and Security; National Nuclear Security Administration; and the DOE Program Offices impacted by a PII breach when the PII breach is significant, crosses DOE organizational boundaries, or as needed. The PIRT will coordinate with the Office of Inspector General (IG) to ensure significant PII breaches involving alleged or suspected crimes are reviewed for potential IG investigation</p> <p>The following considerations will apply in determining the impact of a PII breach resulting in lost, stolen or improperly accessed data:</p> <p>(a) the nature and content of the data (e.g., the data elements involved, such as name, Social Security number and/or date of birth, etc.);</p> <p>(b) the ability of an unauthorized party to use the data, either by itself or in conjunction with other data or applications generally available, to commit identity theft or otherwise misuse the data to the</p>	<p>Renumbered to 1.b.-c.</p> <p>b. <u>Initial Assessment of Reported Breach Involving PII.</u></p> <p>(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.</p> <p>(2) The assessment will determine whether further technical investigation and/or risk assessment is needed to determine the impact of the breach.</p> <p>(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.</p> <p>Examples of mitigating factors include, but are not limited to:</p> <p>(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;</p>

Page	Paragraph	Changed	To
		<p>disadvantage of the record subjects;</p> <p>(c) ease of logical data access to the data given the degree of protection for the data (e.g., unencrypted, plain text, etc.);</p> <p>(d) ease of physical access to the data (e.g., the degree to which the data is readily available to unauthorized access);</p> <p>(e) evidence indicating that the data may have been the target of unlawful acquisition;</p> <p>(f) evidence that the same or similar data had been acquired from other sources improperly and used for identity theft;</p> <p>(g) whether notification to affected individuals through the most expeditious means available is warranted; and</p> <p>(h) whether further review and identification of systematic vulnerabilities or weaknesses and preventive measures are warranted.</p> <p>5. Upon conclusion of any risk analysis by the party leading the investigative effort (i.e. respective Under Secretary, his or her designees, or the PIRT), if there is a finding of reasonable risk for potential misuse of any PII involved, that information along with any supporting material will be shared with both the Senior Agency Official for Privacy and the Chief Information Officer.</p> <p>6. If the Senior Agency Official for Privacy and the Chief Information Officer concur that the data breach does not pose a reasonable risk of harm, the Department will take no further action.</p> <p>7. Conversely, if there is no concurrence, both parties will</p>	<p>(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;</p> <p>(c) An employee knowingly sends an email attachment containing their own sensitive PII unencrypted outside of the DOE IT network; and</p> <p>(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.</p> <p>(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).</p> <p>(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.</p>

Page	Paragraph	Changed	To
		<p>present their views to the Deputy Secretary, who will then decide what, if any, further action is necessary.</p>	<p>(6) The SAOP will determine if the breach meets the criteria of a Major Incident.</p> <p>(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.</p> <p>b. <u>Escalation and Convening of the Privacy Incident Response Team.</u></p> <p>(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.</p> <p>(2) The PIRT will:</p> <p>(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;</p> <p>(b) Coordinate with the IG to ensure significant PII breaches involving alleged or suspected crimes are reviewed for potential IG investigation;</p> <p>(c) Conduct and document an assessment of the risk of harm to individuals impacted or potentially impacted by the breach of PII, based</p>

Page	Paragraph	Changed	To
			on the factors outlined in internal guidance documents.
App B B-3	1.d.-k.	<p>Was 8.-12.</p> <p>8. The Senior Agency Official for Privacy may provide notice to subjects of a data breach and/or offer them Credit Protection Services prior to the completion of any risk analysis. This decision will likely hinge upon the information available to the Department at the time of the data breach, and whether the information suggests there is an immediate and substantial risk of identity theft or other harm.</p> <p>9. The Head of the Departmental Element in which the breach occurred will provide notification to the affected individuals once there is a finding by the PIRT that a reasonable risk exists for potential misuse of any sensitive personal information involved in the data breach. The notification will be signed, and include the following elements as appropriate:</p> <ul style="list-style-type: none"> <li>a. a brief description of what happened, including the dates of the data breach and of its discovery, if known;</li> <li>b. to the extent possible, a description of the personnel information that was involved (e.g., full name, Social Security number, date of birth, home address, account numbers, etc.);</li> <li>c. a brief description of actions taken by the Department to investigate, mitigate losses and protect against any further breach of data;</li> <li>d. contact procedures to ask further questions or learn</li> </ul>	<p>Renumbered to 1.d.-k.</p> <p>d. <u>Individual Notification Procedures and Timelines.</u></p> <ul style="list-style-type: none"> <li>(1) When breaches involve less than 1,000 affected or potentially affected individuals, the CPO and SAOP will determine whether notification is appropriate.</li> <li>(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.</li> <li>(3) The SAOP will advise the Secretary on matters including, but not limited to: <ul style="list-style-type: none"> <li>(a) Whether the Department should provide credit monitoring or identify restoration services to affected or potentially affected individuals;</li> <li>(b) Which Department office or Element should have financial responsibility for the costs of breach</li> </ul> </li> </ul>

Page	Paragraph	Changed	To
		<p>additional information, including a toll-free telephone number, email address, web site, and/or postal address;</p> <p>e. steps that individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts, if appropriate, and instructions for obtaining other credit protection services (NOTE: Alerts may include key changes to fraud reports and on-demand personal access to credit reports and scores); and</p> <p>f. a statement of whether the information was encrypted or protected by other means, when it is determined such information would be beneficial and would not compromise the security of any Departmental systems.</p> <p>10. When there is insufficient or inaccurate contact information that precludes written notification to an affected individual, an alternative form of written notice may be provided.</p> <p>a. This alternative notice may include a conspicuous posting on the home page of the Department's web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals are likely to reside.</p> <p>b. The media notice will include a toll-free telephone number for an individual to contact in order to learn whether or not his/her personal information is</p>	<p>notification and corrective services; and</p> <p>(c) Whether informal, courtesy notification should be provided to OMB or Congressional committees in advance of the Department providing formal notice.</p> <p>(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.</p> <p>(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.</p> <p>(a) Preliminary notice will be provided in accordance to the Element's SAOP approved breach response plan.</p> <p>(b) Preliminary and informal notice may be</p>

Page	Paragraph	Changed	To
		<p>possibly included in the data breach.</p> <p>11. When the SAOP determines that urgent action is required because of possible imminent misuse of PII, the SAOP may provide information to affected individuals by telephone or other means, as appropriate.</p> <p>12. Notwithstanding the foregoing requirements, notification may be delayed upon 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.</p> <p>a. A lawful request should be made in writing to the Secretary of Energy or SAOP by the Federal agency responsible for the investigation regarding security concerns or data recovery efforts that may be adversely affected by providing notification.</p> <p>b. The SAOP must be notified of a delay notification request.</p> <p>c. Any lawful request for delay in notification must state 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.</p> <p>d. Any delay should not increase risk or harm to any affected individuals.</p> <p>e. The Secretary or other Agency official designated by the Secretary will keep the Senior Agency Official for</p>	<p>provided via an in-person meeting, by telephone, or by another appropriate alternative.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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.)</p> <p>(8) The SAOP may delegate the responsibility for providing formal written</p>



Page	Paragraph	Changed	To
		<p>Privacy and the Chief Information Officer informed on the status of any investigation or recovery efforts.</p>	<p>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.</p> <p>(9) The SAOP reserves the ability to elevate notification of an Element-based breach for handling by an appropriate Department component at his discretion.</p> <p>e. <u>Options for Corrective Services to Potentially Impacted Individuals.</u></p> <p>(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.</p> <p>(2) The official authorized to determine whether to provide these services depends on the size of the breach:</p> <p>(a) For breach affecting or potentially affecting less than 1,000 individuals, the SAOP will determine whether and what services will be provided;</p> <p>(b) For breach affecting or potentially affecting more than 1,000 individuals, the SAOP</p>



Page	Paragraph	Changed	To
			<p>will make recommendations to the Secretary (or his/her designee) on what services should be provided to individuals, if any.</p> <p>f. <u>Individual Notification Requirements and Methods.</u></p> <p>(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:</p> <ul style="list-style-type: none"> <li>(a) The source of the notification;</li> <li>(b) The timeliness of the notification;</li> <li>(c) The content of the notification;</li> <li>(d) The method of notification; and</li> <li>(e) Any special circumstances.</li> </ul> <p>(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:</p> <ul style="list-style-type: none"> <li>(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</li> </ul>

Page	Paragraph	Changed	To
			<p>or without password protection) outside of the Department's IT network firewall; or</p> <p>(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.</p> <p>(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.).</p> <p>(4) Automatic notification will be made under the same timelines established above.</p> <p>g. <u>Public Announcements and Media Notification.</u></p> <p>(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</p>

Page	Paragraph	Changed	To
			<p>national security), and the President of the National Treasury Employees Union (NTEU) (other appropriate union representatives).</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(3) Use of a public awareness campaign may also assist</p>

Page	Paragraph	Changed	To
			<p>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.</p> <p>h. <u>Notification of Congress and the White House.</u></p> <p>(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.</p> <p>(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.</p> <p>i. <u>Factors Warranting Delayed Notification of Potentially Affected Individuals.</u></p> <p>(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</p>

Page	Paragraph	Changed	To
			<p>harm to any affected or potentially affected individuals.</p> <p>(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:</p> <p>(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;</p> <p>(b) The lawful or authorized reason for the requested delay; and</p> <p>(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.</p> <p>(3) The SAOP will submit their recommendation, along with the DOE Element's written request, to the Secretary for a final decision.</p>
App B B-8	1.j.	Added.	<p><u>DOE Component/Element/Office-specific Breach Response Plan.</u></p> <p>(1) Secretarial Officers, Heads of Departmental Elements, Heads of Program Offices, and Heads of Field Elements may elect to develop an Element-specific</p>

Page	Paragraph	Changed	To
			<p>or site-specific breach response plan <u>consistent</u> with the Appendix (i.e., the Department's breach response plan), OMB Memorandum 17-12, and applicable law.</p> <p>(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.</p>
App B B-8	1.k.-l.	<p>Was 13.-14.</p> <p>13. Individuals who routinely access PII and their supervisors must sign a document annually describing their responsibilities and the consequences for failure to protect PII.</p> <p>14. Departmental Elements and their sites should maintain a log which tracks all activities—including dates and times of events, decisions and corrective actions—for incidents involving breaches of PII.</p>	<p>k. <u>Tracking Breach Response and Notification Metrics.</u></p> <p>(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.</p> <p>(2) Departmental Components and their offices are required to track all activities for breaches of PII, including:</p> <p>(a) Dates and times of reported breaches;</p> <p>(b) Element-level decisions;</p> <p>(c) Public notifications;</p> <p>(d) Local corrective actions; and</p> <p>(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).</p> <p>l. <u>Annual Readiness Requirements for Breach Response.</u></p>

Page	Paragraph	Changed	To
			<p>(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.</p> <p>(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.</p> <p>(3) Completion of Mandatory Annual Privacy Training.</p> <p>(a) All DOE employees with access to DOE Enterprise IT networks must complete mandatory Privacy Awareness training.</p> <p>(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.</p>
App B	15	The Departmental Element program responsible for the breach of PII shall	Removed.

Page	Paragraph	Changed	To
B-9		incur and be responsible for all costs associated with remediation including notification of affected or potentially-affected individuals.	
Att 1 Page 1	CRD Introduction	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 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.
Att 1 Page 1	1.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 Office of Management and Budget (OMB) directives.	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.
Att 1 Page 1	1.b.(2)	Added.	reporting suspected or confirmed breach of PII; and
Att 1 Page 1	1.b.(2)	Renumbered.	1.b.(3)
Att 1 Page 1	1.b.(3)	complying with the Privacy Act.	complying with the Privacy Act, when required.



Page	Paragraph	Changed	To
Att 1 Page 1	2.b.(3)	report any known or suspected loss of control or unauthorized disclosure of PII	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.
Att 1 Page 2	2.b.(4)	Added.	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.
Att 1 Page 2	2.b.(4)-(7)	Renumbered.	2.b.(5)-(8)
Att 1 Page 2	2.c.	Ensure that contractor employees complete the Annual Privacy Training and sign the completion certificate acknowledging their responsibility for maintaining and protecting Privacy Act information prior to being authorized access to all information systems.	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.
Att 1 Page 2	2.d.	Ensure contractor employees are cognizant of the fact that all personal information collected, maintained, used, or disseminated on behalf of the Agency must be maintained in a Privacy Act SOR.	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.

Page	Paragraph	Changed	To
Att 1 Page 2	2.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	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
Att 1 Page 2	2.g.	Added.	Allow and cooperate with inspection or investigation to determine compliance with this CRD