U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 206.5

Approved: 10-9-07
Expires: 10-9-08

SUBJECT: RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION

1. PURPOSE. To comply with Office of Management and Budget (OMB) Memorandum (M) 07-16, "Safeguarding Against and Responding to Breaches of Personally Identifiable Information." This Notice concerns actions to address data breaches of personally identifiable information (PII) that is collected, processed or maintained by DOE. Data includes but is not limited to PII that is stored on paper records, stored and/or transmitted through DOE computer systems, and sensitive data owned by DOE that is properly stored on non-DOE computer systems. This Notice does not supersede or supplant the requirements imposed by other laws, such as the Privacy Act of 1974.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. DOE Elements. Except for the exclusions in paragraph 3c, this Notice applies to Departmental elements, including those created after the Order is issued.. (Go to http://www.directives.doe.gov/pdfs/reftools/org-list.pdf for the most current listing of Departmental elements.)

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

   b. DOE Contractors. Except for exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Notice that will apply to contracts that include the CRD. The CRD must be included in site or facility management contracts that involve contractor access to or responsibility for DOE related (PII).

   c. Exclusions. None.

4. REQUIREMENTS.

   a. Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees who collect, maintain, use, or disseminate PII on behalf of the Department will immediately report the same 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*, dated 12-4-06, and further explained in DOE CIO Guidance CS-9, *Incident Management* and CIO Guidance CS-38A, *Protection of Sensitive Unclassified Information, Including Personally Identifiable Information.*

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

(1) loss of control of employee information consisting of names and social security numbers (including temporary loss of control);

(2) loss of control of Department credit card holder information;

(3) loss of control of PII pertaining to the public;

(4) loss of control of security information (e.g., logons, passwords, etc.);

(5) incorrect delivery of sensitive PII;

(6) theft of PII; and

(7) unauthorized access to PII stored on Department operated web sites.

c. Reports of PII breaches will be transmitted via the DOE Computer Incident Advisory Capability (CIAC) in accordance with applicable Deputy Secretary or Under Secretary policies and procedures.

d. Within one hour of receiving the PII breach report, the CIAC will notify the U.S. Computer Emergency Response Team (US CERT) of the breach, as set forth in OMB Directive 06-19 and in accordance with current incident reporting processes. Additionally, the CIAC will notify the Department's Senior Agency Official for Privacy and other senior officials in accordance with current procedures.

e. The Senior Agency Official for Privacy will consult with the Deputy Secretary and Under Secretaries and other senior agency and contractor officials to ensure that a determination has been made regarding the impact of the breach as directed below.

f. Additionally, the Senior Agency Official for Privacy may convene a DOE Privacy Incident Response Team (PIRT) comprised of the Senior Agency Official for Privacy, and representatives from the Offices of the Chief Information Officer; Public Affairs; General Counsel; Management; Health, Safety and Security; National Nuclear Security Administration; and the program offices impacted by a PII breach when the PII breach is significant, crosses DOE organizational

boundaries, or as needed. The following considerations will apply determining the impact of a PII breach resulting in lost, stolen or improperly accessed data:

(1) 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.);

(2) 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 disadvantage of the record subjects;

(3) ease of logical data access to the data given the degree of protection for the data (e.g., unencrypted, plain text, etc.);

(4) ease of physical access to the data (e.g., the degree to which the data is readily available to unauthorized access);

(5) evidence indicating that the data may have been the target of unlawful acquisition;

(6) evidence that the same or similar data had been acquired from other sources improperly and used for identity theft;

(7) whether notification to affected individuals through the most expeditious means available is warranted; and

(8) whether further review and identification of systematic vulnerabilities or weaknesses and preventive measures are warranted.

g. Upon conclusion of any risk analysis by the party leading the investigative effort (i.e., respective Under Secretary, his or her designees, or the DOE 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.

h. 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.

i. Conversely, if there is no concurrence, both parties will present their views to the Deputy Secretary, who will then decide what, if any, further action is necessary.

j. 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.

k. The head of the Departmental element in which the breach occurred will provide notification to the record subjects once there is a finding by the DOE 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:

(1) a brief description of what happened, including the dates of the data breach and of its discovery, if known;

(2) 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.);

(3) a brief description of actions taken by the Department to investigate, mitigate losses and protect against any further breach of data;

(4) contact procedures to ask further questions or learn additional information, including a toll-free telephone number, email address, web site, and/or postal address;

(5) 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

(6) 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.

l. When there is insufficient or inaccurate contact information that precludes written notification to an individual subject to a data breach, an alternative form of written notice may be provided.

(1) 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.

(2) 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 possibly included in the data breach.

m. When the Secretary or the Secretary's designee determines that urgent action is required because of possible imminent misuse of PII, the Secretary may provide information to individuals by telephone or other means, as appropriate.

n. 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.

(1) A lawful request should be made in writing to the Secretary of Energy, or designee, by the Federal agency responsible for the investigation, security concerns, or data recovery efforts that may be adversely affected by providing notification.

(2) The Senior Agency Official for Privacy and the Chief Information Officer must be notified of a delay notification request.

(3) Any lawful request for delay in notification must state an estimated date after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover data.

(4) Any delay should not exacerbate risk or harm to any affected individuals.

(5) The Secretary or other Agency official designated by the Secretary will keep the Senior Agency Official for Privacy and the Chief Information Officer informed on the status of any investigation or recovery efforts.

o. Individuals who routinely access PII and their supervisors must sign a document annually describing their responsibilities for and the consequences for failure to protect PII.

5. RESPONSIBILITIES.

a. Secretarial Officers or Senior Level Designees.

(1) Ensure that personnel minimize the collection of PII to only that which is required to conduct business operations.

(2) Ensure that PII is protected by safeguards that provide security, confidentiality and privacy.

(3) Ensure that all individuals who routinely access PII and their supervisors annually sign a document that acknowledges their responsibilities regarding PII and the consequences for failure to protect PII.

(4) Use encryption, authentication, and other security controls to make PII unusable in electronic form by unauthorized individuals.

(5) Require that in the event of an actual or suspected breach, employees, contractors or appropriate subcontractors, immediately report the incident to the CIAC.

(6) Ensure that procedures are followed in accordance with OMB M-07-16 and this Notice to assess the impact of PII data breaches and ensure appropriate action is taken.

(7) Identify contracts that are subject to this Notice, and notify the appropriate contracting officers of the need to incorporate the requirements of this Notice into said contracts.

b. Director, Office of Management.

(1) Serves as the Senior Agency Official for Privacy.

(2) Directs the Department's program for the protection, reporting and responses to known or suspected PII breaches.

(3) Ensures that the Department's implementation of information privacy protection is in accordance with OMB M-07-16.

(4) Addresses potential privacy issues that impact the Department's programs by directing various groups established to address such matters, such as the DOE Privacy Incident Response Team.

(5) Conducts an annual risk assessment to identify areas of privacy-related vulnerabilities and risks that are common across the Department.

c. Chief Information Officer.

(1) Supports the efforts of the Senior Agency Official for Privacy to ensure implementation of OMB M-07-16.

(2) Provides technical support and/or recommendations to the Secretary, Deputy Secretary, Senior Agency Official for Privacy, and DOE Senior Management Officials regarding electronic, or computer related, sources of PII data and access.

(3) Provides the Department's cyber incident handling process, currently CIAC, to serve as the central point of contact for DOE employees, contractors and their subcontractors for reports of all suspected or confirmed PII losses or theft regardless of form (e.g., electronic, paper, etc,).

(4) Notifies the US CERT within the prescribed time of one hour after receiving a report of a suspected or confirmed PII loss or theft.

(5) Provides to contractor management guidance regarding technical particulars and strategies for multi-layer cyber security protection.

d. DOE Privacy Incident Response Team provides advice, mitigation strategies and analyses to the Senior Agency Officer for Privacy as needed.

e. Contracting Officers.

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

(2) Ensure that contracting officer's representatives (CORs) and/or contracting officer's technical representatives (COTRs) are aware of provisions within this Notice and any changes to their respective contracts.

(3) In the case of loss of property, contact the Organizational Property Management Officer (OPMO).

(4) Provide appropriate guidance to contractors on their responsibilities to safeguard Government property and PII.

f. DOE Employees Who Collect, Maintain, Use, or Disseminate PII on Behalf of the Department.

(1) Immediately report all suspected or known breaches of PII in accordance with their organization's existing cyber incident reporting policies and procedures.

(2) Protect the security of PII to—

(a) ensure its accuracy, relevance, timeliness and completeness;

(b) avoid unauthorized disclosure; and

(c) ensure that no system of records concerning individuals, no matter how insignificant or specialized, is maintained without public notice.

6. REFERENCES

a. OMB M-07-16, "Safeguarding Against and Responding to Breaches of Personally Identifiable Information."

b. Public Law (P.L.) 107-217, Federal Information Security Management Act of 2002 (FISMA).

c. P.L. 93-579, Privacy Act of 1974.

d. DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

e. DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06.

f. DOE O 580.1, *Department of Energy Personal Property Management Program*, dated 5-20-02.

7. DEFINITIONS.

a. Access. The ability or opportunity to gain knowledge of personally identifiable information.

b. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

c. Breach. The loss of control, compromise, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to personally identifiable information, whether physical or electronic.

d. Data breach assessment. The process used to determine if a data breach has resulted in the misuse of personally identifiable information.

e. Data breach analysis. The process used to conduct an overall review of what, if any, information or systems were compromised, the significance of such losses or intrusions, and how to prevent future occurrences.

f. Department. Department of Energy, including the National Nuclear Security Administration, contractors and their subcontractors.

g. Harm. Fiscal or physical harm, embarrassment, coercion that can result from the unauthorized disclosure of personal information, and the security risk, identity theft or coercion or other adverse action that can result from information that can be created through manipulation of information obtained through an unauthorized disclosure.

h. 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."

i. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

j. Individual. A citizen of the United States or an alien lawfully admitted for permanent residence in accordance with the Privacy Act of 1974.

k. Personally Identifiable Information (PII). Any information 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, etc., and including any other personal information that is linked or linkable to a specific individual.

l. Information system. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

m. Senior Agency Official for Privacy. A DOE employee designated in writing by the Secretary or Deputy Secretary as charged with overall responsibility and authority for protecting and reporting PII breaches for the Department.

n. Unauthorized access. Viewing, obtaining, or using data from an electronic information system that contains sensitive personal information in any form or in any Department of Energy information system.

8. CONTACT. Questions concerning this Notice should be addressed to the Office of Management at (202) 586-2550.

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

CONTRACTOR REQUIREMENTS DOCUMENT

DOE N 206.5, RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION

This contractor requirements document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors. Contractors must comply with the requirements listed in the CRD to the extent set forth in their contracts.

Regardless of who performs the work, contractors subject to this CRD are responsible for compliance with the requirements of the CRD and are also responsible for flowing down requirements of the CRD to subcontractors at any tier to the extent necessary to ensure the contractors' compliance with the requirements.

1. PURPOSE.

   a. It is necessary for the contractor to assist DOE in meeting DOE responsibility to comply with Office of Management and Budget Memorandum M-07-16, "Safeguarding Against and Responding to Breaches of Personally Identifiable Information."[1]

   b. The contractor is required to take actions to address data breaches of personally identifiable information (PII) that is collected, processed or maintained by DOE contractors.

   c. The subject data includes but is not limited to PII that is stored on paper records, stored and/or transmitted through DOE computer systems, and sensitive data owned by DOE that is properly stored on non-DOE computer systems. This CRD does not supersede or supplant the requirements imposed by other laws, such as the Privacy Act of 1974.

2. REQUIREMENTS.

   a. Contractors will assess computer systems to ensure that—

      (1) classified systems are protected using multi-layer protection and

      (2) systems are protected against both outsider and insider threats.

   b. Contractor management will consult with the DOE Chief Information Officer regarding technical particulars and strategies for multi-layer cyber security protection.

1 OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," 22 May 2007.

c. Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, contractors who collect, maintain, use, or disseminate PII on behalf of the Department will immediately report the same in accordance with existing cyber incident reporting processes, which have been established in senior DOE management program cyber security plans (PCSPs).

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

(1) loss of control of employee information consisting of names and social security numbers (including temporary loss of control);

(2) loss of control of Department credit card holder information;

(3) loss of control of PII pertaining to the public;

(4) loss of control of security information (e.g., logons, passwords, etc.);

(5) incorrect delivery of sensitive PII;

(6) theft of PII; and

(7) unauthorized access to PII stored on Department operated web sites.

e. Reports of PII breaches will be transmitted via the Department of Energy Computer Incident Advisory Capability, or CIAC. [See DOE O 205.1A, *Department of Energy Cyber Security Management*]

3. DEFINITIONS.

a. Access. The ability or opportunity to gain knowledge of personally identifiable information.

b. Breach. The loss of control, compromise, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to personally identifiable information, whether physical or electronic.

c. Personally Identifiable Information (PII). Any information 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, etc., and including any other personal information that is linked or linkable to a specific individual.