



Overview of Personally Identifiable Information (PII) Incident Activities

May 7, 2008

**Ray Holmer, Director
Office of Information Management
Office of Resource Management
Office of Health, Safety, and Security
U.S. Department of Energy**



Agenda



- Policies and Regulations
- Definition of PII
- Applicability
- Reporting Requirements
- Internal Actions / Requirements
- Liabilities
- Questions



Policies and Regulations



- Privacy Act of 1974
- Federal Information Security Management Act (FISMA) of 2002
- Health Insurance Portability and Accountability Act (HIPAA)
- Office of Management and Budget (OMB) Memorandum (M) 07-16, "Safeguarding Against and Responding to Breaches of Personally Identifiable Information."
- DOE N 206.5 "Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information"



Policies and Regulations



- All systems (paper based and IT based) and data collections / repositories required to have a:
 - Privacy Impact Assessment that details the data collection and the measures and controls governing the protection and release of that data
 - System of Records Notice (SORN) that defines the data collection and details the uses of the data and the purposes and to whom the data can be released. Some examples of SORNs covering PII are:
 - DOE-43, “Personal Security Clearance Files”
 - DOE-51, “Employee and Visitor Access Control Records” covers access control records and badge systems (paper and IT)
 - DOE–63, “Personal Identity Verification (PIV) Files” covers records generated or used in conjunction with HSPD-12



Definition of 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.



Applicability



- 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 in non-DOE computer systems.



Reporting Requirements



- Types of breaches that must be reported include, but are not limited to the following:
 - loss of control of employee information consisting of names and social security numbers (including temporary loss of control);
 - loss of control of Department credit card holder information;
 - loss of control of PII pertaining to the public;
 - loss of control of security information (e.g., logons, passwords, etc.);
 - incorrect delivery of sensitive PII;
 - theft of PII; and
 - unauthorized access to PII stored on Department operated web sites.



Reporting Requirements



- PII Breaches must be reported within 1 hour of discovery
- 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.
- 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
- Additional Notifications include
 - DOE Senior Management
 - Office of Management and Budget
 - House and Senate Committees
 - Other Government Agencies with an equity



Internal Actions Requirements



- Program Offices are responsible for compiling a report that contains:
 - a brief description of what happened, including the dates of the data breach and of its discovery, if known;
 - a description of the personnel information that was involved (e.g., full name, social security number, date of birth, home address, account numbers, etc.);
 - a brief description of actions taken by the Department to investigate, mitigate losses and protect against any further breach of data;
 - contact procedures to ask further questions or learn additional information, including a toll-free telephone number, email address, web site, and/or postal address;
 - 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
 - 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.



Internal Actions Requirements



- Risk Analysis / DOE Privacy Impact Response Team (PIRT)
 - 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.);
 - 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;
 - ease of logical data access to the data given the degree of protection for the data (e.g., unencrypted, plain text, etc.);
 - ease of physical access to the data (e.g., the degree to which the data is readily available to unauthorized access);
 - evidence indicating that the data may have been the target of unlawful acquisition;
 - evidence that the same or similar data had been acquired from other sources improperly and used for identity theft;
 - whether notification to affected individuals through the most expeditious means available is warranted; and
 - whether further review and identification of systematic vulnerabilities or weaknesses and preventive measures are warranted.



Liabilities



- The Department or Program Office may be responsible for:
 - Providing credit monitoring service for 1 year
 - Legal fees of individuals whose PII was lost / stolen
 - Civil Law Suits
 - Criminal Prosecution (negligence)



Questions



Questions ??