

**U.S. Department of Energy  
Cyber Security Program**

**PROTECTION OF SENSITIVE  
UNCLASSIFIED INFORMATION,  
INCLUDING PERSONALLY IDENTIFIABLE  
INFORMATION  
Guidance**



November 2006

*This Guidance document was  
developed and issued outside of  
the Departmental Directives*

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance identifies controls to ensure adequate protection of sensitive unclassified information (SUI), including personally identifiable information (PII). It applies requirements and guidance from Office of Management and Budget (OMB) memorandum, M-06-16, Protection of Sensitive Agency Information, and the sections of OMB memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, pertaining to the protection of PII.

The DOE CIO will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

This Guidance addresses protection of SUI, including PII, associated with all information systems operated by the Department and its contactors.

Processes and criteria for privacy impact assessments are outside the scope of this document. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, provides the criteria for determining whether an information system requires a privacy impact assessment as well as the requirements for performing the assessment.

3. CANCELLATIONS.

This guidance replaces DOE CIO Guidance CS-38, Protection of Personally identifiable Information Guidance, July 20, 2006.

4. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, Primary Department of Energy Organizations to Which DOE CIO Guidance CS-38A is Applicable.

This Guidance applies to all DOE subordinate organizations and contractors (hereafter called operating units) that use and operate Government-furnished information technology systems for or on behalf of the DOE or host DOE information on their non-Government information technology systems.

This guidance is not applicable to contractors and subcontractors that provide products and services to DOE, operate independent of DOE sites and organizations, or host only DOE-identified public information on their non-Government systems.

Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate operating units, and ensure that those requirements are incorporated into contracts. Senior DOE Management may also identify additional information as SUI that requires this level of protection within their organizations. Attachment 2 is provided to present examples of what is and is not considered PII.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.
- c. DOE Unclassified Systems. Senior DOE Management Program Cyber Security Plans (PCSPs) are to address this Guidance for all systems hosting SUI, including PII. DOE M 471.3-1, Manual for Identifying and Protecting Official Use Only Information, and DOE M 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information Manual, and 15 CFR 730 -774, Export Administration Regulations, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security systems. Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the National Industrial Security Program Operating Manual (NISPOM); the Atomic Energy Act of 1954, which established Restricted Data information; DOE CIO Guidance CS-22, National Security Systems Controls Guidance; and NIST SP 800-59, Guidelines for Identifying an Information System as a National Security System, provides additional guidance for identifying National Security Systems.

## 5. IMPLEMENTATION.

This Guidance is effective upon issuance. Senior DOE Management shall address the criteria in this document within 30 days of its issuance date. If Senior DOE Management cannot address all of the criteria within the 30-day period, Senior DOE Management must notify the DOE CIO and establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance in their PCSP.

6. CRITERIA.

- a. Program Cyber Security Plan. Senior DOE Management PCSPs are to direct operating units to develop, document, and implement policies and procedures for protecting SUI, including PII, in accordance with the following criteria.
- (1) SUI and PII are defined in Section 9 as they are used in this Guidance. Senior DOE Management may extend the definition of SUI to include other types of sensitive information that they determine require this level of protection within their organizations. The definition of PII, provided by OMB, however, should not be modified. Senior DOE Management should interpret this definition by applying the working examples of what is and what is not considered PII provided in Attachment 2 to identify PII within their organizations. Extensions of the definition of SUI must be documented in the Senior DOE Management PCSPs
  - (2) A process to select and train individuals within the operating units to identify SUI.
  - (3) Use of Encryption.
    - (a) Portable/Mobile Devices and Removable Media containing SUI. FIPS 140-2 Level 1 or higher encryption is to be implemented for protection of all SUI on portable/mobile devices and removable media, such as CDROMs or thumb drives. All portable/mobile devices and removable media used by Federal employees and all DOE contractors who support systems that contain DOE SUI should have an installed capability to encrypt all such information.

[Cautionary Note: Cryptographic modules validation certificates issued by the Cryptographic Module Validation Program (including FIPS 140-1, 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until the validation certificate is specifically revoked. The FIPS 140-2 standard also acknowledges the use of cryptography approved by the National Security Agency as an appropriate alternative. Consult FIPS 140-2 for specific guidance.]

The following steps are to be followed to implement this criteria:

- i. Identify all portable/mobile devices that contain SUI. (Note: All portable/mobile devices are assumed to contain PII unless a designated authorizing Federal management official determines there is no PII on the device. A similar process should be established for reviewing SUI, other than PII, that may be on a device. See Section 7 below.)
- ii. Remove SUI from all portable/mobile devices for which its presence is not required.

- iii. Install encryption software for all portable/mobile devices that contain SUI or may contain SUI in the future.
  - iv. Provide user training on the use of the encryption software.
  - v. Direct and enforce the use of the encryption software to protect SUI on all portable/mobile devices.
- (b) Encryption is required for protecting SUI hosted on all portable/mobile devices, desktop computer systems, and any removable media. Encryption of the entire contents of the hard drive(s) of each desktop computer system/workstation (including laptops) is preferred for protection against data theft or loss and additional defense against cyber attacks.
- (c) FIPS 140-2 Level 1, or higher, encryption must be applied during the transmission of all SUI unless communications media can provide an equivalent protection as determined by the DAA. NIST-certified FIPS 140-1 encryption may be used until the NIST certification expires.
- (d) Decryption capabilities or recovery of encryption keys must be available, on request, to law enforcement officials, cyber incident management personnel, and cyber forensics personnel.
- b. Remote Access.
- (1) Two-factor authentication must be used for all remote access to SUI, including PII.
  - (2) Ensure that a time-out function is in place on all information systems supporting remote access to SUI. The time-out function must require re-authentication of remote users if there is a period of 30 minutes or longer of inactivity on user connections to the system.
- c. Management of PII on Portable/Mobile devices and Removable Media
- (1) Establish, document, and implement procedures so that any files containing PII on portable/mobile devices or removable media are deleted within 90 days of their creation, or that the approval for continued use of these files is documented<sup>1</sup>.
  - (2) Document the timely review of PII on portable/mobile devices and removable media in accordance with Senior DOE Management procedures.

---

<sup>1</sup> Owners of portable/mobile devices and removable media and their supervisors should be involved in the review on the content of their devices that they use, since they are most familiar with such content. The review should be thoroughly and accurately documented to provide sufficient information to properly determine the disposition of the content of each device.

d. Reporting of Cyber Security Incidents Involving PII

- (1) Establish, document, and implement procedures for reporting cyber security incidents related to PII in accordance with the processes and time frames outlined in DOE CIO Guidance CS-9, Incident Management.
- (2) Develop processes to notify the Information Owner once it has been determined that confidentiality of PII has been compromised.
- (3) Ensure that all suspected or confirmed cyber security incidents involving media containing PII (including the physical loss/theft of computing devices) are reported to the DOE Cyber Incident Advisory Capability (CIAC) within 45 minutes of discovery. CIAC will report to the US-Computer Emergency Readiness Team (US-CERT) in accordance with its procedures.
- (4) When reporting possible cyber security incidents involving PII, there should be sufficient reason to believe that a security breach has occurred and that PII is likely to have been involved. Otherwise, the incident should be reported following documented procedures for reporting all cyber security incidents.
- (5) Reports to CIAC should be made via the CIAC AWARE portal, or alternatively by email to [ciac@ciac.org](mailto:ciac@ciac.org), phone to 925-422-8193, or fax to 925-423-8002.

e. Additional Criteria for National Security Systems. Security controls for SUI are to comply with the controls identified for the Confidential/Secret Information Group as identified in DOE M 205.1-X; National Security Systems Controls Manual.

7. RESPONSIBILITIES.

Heads of Departmental Elements have been authorized<sup>2</sup> to determine whether data on portable/mobile devices and removable media contain PII (Recommendation 1 in OMB M-06-16). This authorization may be further delegated to Federal management officials.

8. REFERENCES.

References are defined in DOE CIO Guidance CS-1, Management, Operational, and Technical Controls.

---

<sup>2</sup> This designation was made in a memorandum from the Deputy Secretary to Heads of Departmental Elements dated August 17, 2006.

## 9. DEFINITIONS.

Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, Management, Operational, and Technical Controls Guidance. The following terms apply specifically to this Guidance.

**Cyber Security Incident**—Any adverse event that threatens the security of information resources, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Adverse events include, but are not limited to, attempts (successful or persistent) to gain unauthorized access to an information system or its data; unwanted disruption or denial of service; unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent. Examples include insertion of malicious code (for example, viruses, Trojan horses, or back doors), unauthorized scans or probes, successful or persistent attempts at intrusion, and insider attacks.

**Personally Identifiable Information (PII) (as defined by OMB)** - Any information about an individual maintained by an Agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual’s identity, such as their name, social security numbers, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. In some instances PII overlaps with Privacy Act information.

**Remote Access** - Any access from outside the accreditation boundary of the information system.

**Sensitive Unclassified Information (SUI)** - Unclassified information requiring protection mandated by policy or laws, such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Power Information (NNPI), Personally Identifiable Information (PII), and other information specifically designated as requiring SUI protection, such as information identified under Cooperative Research and Development Agreements (CRADA).

## 10. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

Attachment 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO  
WHICH DOE CIO Guidance CS-38A IS APPLICABLE

Office of the Secretary  
Office of the Chief Financial Officer  
Office of the Chief Information Officer  
Office of Civilian Radioactive Waste Management  
Office of Congressional and Intergovernmental Affairs  
Departmental Representative to the Defense Nuclear Facilities Safety Board  
Office of Economic Impact and Diversity  
Office of Electricity Delivery and Energy Reliability  
Office of Energy Efficiency and Renewable Energy  
Energy Information Administration  
Office of Environment, Safety and Health  
Office of Environmental Management  
Office of Fossil Energy  
Office of General Counsel  
Office of Health, Safety, and Security  
Office of Hearings and Appeals  
Office of Human Capital Management  
Office of the Inspector General  
Office of Intelligence and Counterintelligence  
Office of Legacy Management  
Office of Management  
National Nuclear Security Administration  
Office of Nuclear Energy  
Office of Policy and International Affairs  
Office of Public Affairs  
Office of Science  
Bonneville Power Administration  
Southeastern Power Administration  
Southwestern Power Administration  
Western Area Power Administration

Attachment 2

DOE Working Examples of Personally Identifiable Information (PII)

WHAT IS PII:

- Social Security Numbers in any form are PII
- Place of Birth associated with an individual
- Date of birth associated with an individual
- Mother's maiden name associated with an individual
- Biometric record associated with an individual
- Fingerprint
- Iris scan
- DNA
- Medical history information associated with an individual
- Medical conditions, including history of disease
- Metric information, e.g. weight, height, blood pressure
- Criminal history associated with an individual
- Employment history and other employment information associated with an individual
- Ratings
- Disciplinary actions
- Performance elements and standards (or work expectations) are PII when they are so intertwined with performance appraisals that their disclosure would reveal an individual's performance appraisal.
- Financial information associated with an individual
- Credit card numbers
- Bank account numbers
- Security clearance history or related information (Not including actual clearances held)

## WHAT ISN'T PII:

- Phone numbers (Work, Home, Cell)
- Street addresses (Work and personal)
- Email addresses (Work and personal)
- Digital pictures
- Birthday cards
- Birthday emails
- Medical information pertaining to work status (X is out sick today)
- Medical information included in a health or safety report
- Employment information that is not PII even when associated with a name
- Resumes, unless they include an SSN
- Present and past position titles and occupational series
- Present and past grades
- Present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials)
- Present and past duty stations and organization of assignment (includes room and phone numbers, organization designations, work e-mail address, or other identifying information regarding buildings, room numbers, or places of employment)
- Position descriptions, identification of job elements, and those performance standards (but not actual performance appraisals) that the release of which would not interfere with law enforcement programs or severely inhibit agency effectiveness
- Security clearances held
- Written biographies (like the ones used in pamphlets of speakers)
- Academic credentials
- Academic credentials, e.g. Ph.D, MS, BS, AA
- Schools attended
- Major or area of study
- Personal information stored by individuals about themselves on their assigned workstation or laptop (unless it contains an SSN)