Cyber Security Technical and Management Requirements

Protection of Sensitive Unclassified Information, Including Personally Identifiable Information (TMR-22)
October 16, 2007

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs). This TMR provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

This TMR identifies controls to ensure adequate protection of sensitive unclassified information (SUI), including personally identifiable information (PII), associated with all information systems operated by the Department and its contactors. 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. Processes and criteria for privacy impact assessments are outside the scope of this document.

Cancellations

This TMR replaces DOE CIO Guidance CS-38A, *Protection of Sensitive Unclassified Information, Including Personally Identifiable Information Vulnerability Management*, dated November 2006.

Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

Requirements

TMR-22-1, Senior DOE Management SUI Management Program

Senior DOE Management is responsible for developing, documenting, and implementing a program for managing SUI, including PII, for all operating units, programs, and

systems. The Senior DOE Management SUI Management program is to be documented in the PCSP and include the following requirements.

1. SUI is defined below; 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. Extensions of the definition of SUI must be documented in the PCSP.

   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).

2. The OMB definition of PII is included below. This definition is not to be modified by Senior DOE Management or its operating units. Senior DOE Management should interpret this definition by applying the working examples of what is and what is not considered PII provided in Attachment 1 to identify PII within their organizations.

   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.

3. Use of Encryption.

   a. Federal Information Processing Standard (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 containing SUI. All such information on portable/mobile devices and removable media that contain SUI used by Federal employees and all DOE contractors should be encrypted.

      [Cautionary Note: Cryptographic modules validation certificates issued by the Cryptographic Module Validation Program (including FIPS 140-1, 140-2, and future amendments - http://csrc.nist.gov/publications/fips/) 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 requirement.

(1) Define processes for regularly reviewing all portable/mobile devices that contain SUI.

(2) Remove SUI from all portable/mobile devices for which its presence is not required. (See DOE CIO TMR-10, *Media Clearing, Purging, and Destruction.*)

(3) Direct and enforce the use of encryption to protect SUI on all portable/mobile devices.

b. Encryption is required for protecting SUI hosted on all portable/mobile devices and any removable media.

c. 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.

d. Encryption in storage is not required until the file has been removed from storage and returned.

e. 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.

f. Decryption capabilities or recovery of encryption keys must be available, on request, to law enforcement officials, cyber incident management personnel, and cyber forensics personnel.

4. Remote Access (See DOE CIO TMR-19 for general Remote Access requirements.)

a. At least two-factor authentication must be used for all remote access to SUI, including PII.

b. Ensure that a user activity time-out function is in place on all information systems supporting remote access to SUI. The time-out function must require re-authentication, at a minimum, after 30 minutes of inactivity on user connection(s).

5. Management of PII on Portable/Mobile Devices and Removable Media

a. All portable/mobile devices are assumed to contain PII unless a designated authorizing Federal management official determines there is no PII on the device.

b. Establish, document, and implement procedures for regular review of all portable/mobile devices and removable media for PII.

c. Establish, document, and implement procedures for removal of files containing PII that are 90 days or older, unless extended use of such files is approved. Approval for use of files containing PII on portable/mobile devices and removable media for longer than the 90-day period must be documented and is not to exceed a period of 1 year[1].

d. Document the timely review of PII on portable/mobile devices and removable media in accordance with Senior DOE Management procedures.

6. Protection requirements, control procedures, and use of encryption software for SUI, including PII, are to be included in user training.

7. Reporting requirements for cyber security incidents involving PII are described in DOE CIO TMR-9, *Incident Management*.

8. Security controls for SUI on National Security Systems (NSS) are to comply with the highest level controls for the associated NSS and not less than the controls identified for the Confidential/Secret Information Group, at a minimum, as identified in DOE M 205.1-4, *National Security System Manual.*

TMR-22-2, Operating Unit SUI Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, implement, and maintain policies and procedures for protecting SUI, including PII, compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization's environment and specific needs.

[1] 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.

Attachment 1
DOE Working Examples of Personally Identifiable Information (PII)

WHAT IS PII (when associated with an individual):

- Social Security Numbers in any form are PII
- Place of Birth
- Date of birth
- Mother's maiden name
- Biometric record
  - Fingerprint
  - Iris scan
  - DNA
- Medical history information
- 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
- 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
- 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
- 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)