Cyber Security Technical and Management Requirements

Remote Access (TMR-19)
August 10, 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 to be used in preparing each PCSP. This TMR identifies topics concerning remote access that are to be covered in each PCSP, and it provides specific direction applicable to the DOE environment and OMB and NIST guidance, enabling Senior DOE Management to implement a risk-based approach for the use of remote access. The TMR applies to remote access from outside each system's accreditation boundary to all DOE computers and all contractor computers operated or used on behalf of DOE. It should be noted that this definition of remote access is broader than, but inclusive of, that defined by OMB for protection of personally identifiable information. Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

Cancellations

This TMR replaces DOE CIO Guidance CS-24, *Remote Access to DOE Information Systems Guidance*, dated January 2007.

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-19-1, Senior DOE Management Requirements for Remote Access

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing policies, processes, and procedures for allowing access to accredited

systems from outside of the accreditation boundary (remote access[1]) for all operating units, programs, and systems. At a minimum, the Senior DOE Management PCSPs are to include the following.

1. Policies and processes governing the conditions under which remote access can be granted and terminated.

2. Processes and procedures for granting and maintaining remote access privileges that include the following principles.

    a. Remote access user is initially granted and annually revalidated based on authorized business needs, including scientific and other collaborative activities.

    b. Remote user access is based on the concept of least privilege (i.e., remote access must be limited to the minimum privileges required).

3. Rules of behavior and operations and consequences for violating remote access policy and procedures, including the prohibition of entering any classified information on any remote computing resource not approved for such information.

4. Controls and safeguards for any Government-issued cryptographic keys, authentication tokens, or passwords, used for remote access.

5. Processes that ensure that the minimum security controls implemented in an information system are not degraded by allowing remote access.

6. Identification of acceptable types of personal identification for remote access.

    a. Clear-text, reusable passwords for remote access are prohibited. Legacy systems that use clear text passwords (See DOE CIO TMR-11, Password Management) are prohibited from participating in remote access.

    b. Privileged users and administrators are to use multi-factor authentication and utilize a trusted path capability (e.g., Virtual Private Network (VPN), Protected Transmission System (PTS), etc.) for remote access initial sign-on/ logon.

    c. General users accessing unclassified systems containing information for which confidentiality impact is Moderate or High are to use two-factor authentication and a trusted path (e.g., VPN, PTS, transmission media under DOE physical control, etc.) for initial sign-on/ logon.

    d. General users accessing National Security Systems are to use at least two-factor authentication and a trusted path (e.g., VPN, PTS, transmission media under DOE physical control, etc.) for initial sign-on/ logon.

[1] The definition of remote access used in this document differs from that used by the Office of Management and Budget (OMB) in its guidance related to Personally Identifiable Information (PII).

7. An inactivity time-out function is in place on all systems allowing remote access. Re-authentication of remote users is required:

   a. For unclassified systems of Security Category Moderate or High, after a period of inactivity of no greater than 30 minutes; and

   b. For all National Security Systems after a period of inactivity of no greater than 15 minutes.

TMR-19-2, Operating Unit Remote Access Policies and Procedures

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