Cyber Security Technical and Management Requirements

Interconnected Systems Management (TMR-5)
October 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 document provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources. The interface between two systems must be capable of adjudicating the different security policy implementations of the participating information systems. A controlled interface is used to control information flow based on information type; maintain the confidentiality, integrity, and availability of information being transmitted; and provide protection services for the interconnected systems. Information systems implementing controls to protect different information types need additional controls to arbitrate the flow of information between the information systems.

This TMR establishes a risk-based approach to interconnected systems management that is to be covered in each PCSP. It also provides guidance for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Systems*. 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-5, *Interconnection Agreements Guidance*, dated July 28, 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-5-1, Senior DOE Management Interconnection Processes

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing processes for interconnecting information systems to be used by all operating units, programs, and systems. These processes must include the following:

1. Analyze the information types, security controls, and control implementation on the systems to be connected to determine the management and technical interface requirements.
   a. Identify the information types that each system is accredited or will be accredited to process.
   b. Identify any differences in security controls and control implementation between the systems to be connected.
2. Identify and assess additional threats and risk that may result from the interconnection.
3. Identify the method of transmission.
4. Determine controls needed for the interface to provide protection for information to pass through the interface.
5. Determine additional controls resulting from the necessity for a controlled interface.
6. Document the baseline interface technical configuration in the Interconnection Security Agreement (ISA) and management responsibilities in the Memorandum of Understanding (MOU).
7. Identify any additional Certification and Accreditation (C&A) requirements.
8. Approve the MOU and ISA.

TMR-5-2, Interconnection Documentation

The Senior DOE Management PCSP is to specify the contents and format of required documentation for the interconnections to be used by all operating units, programs, and systems. At a minimum, the documentation must include the following:

1. Memorandum of Understanding. The MOU details the management agreement and describes responsibilities between organizations with interconnected information systems. The contents of the MOU must include:
   a. The purpose of the interconnection.
   b. The identification of systems to be interconnected and their accreditation levels.

c. The information intended to flow across the interface and direction of data flow.

d. Responsibilities and processes for mutual management, maintenance, operation, and configuration management for the interface.

e. Responsibilities and processes for disconnection and connection re-establishment.

f. Responsibilities, processes, and methods for mutual incident response and reporting.

g. Responsibilities and processes for establishing cross-domain accounts.

h. Personnel points of contact for both interconnected systems, including the cognizant Designated Approving Authorities (DAAs).

i. Identification of the associated ISA.

2. Interconnection Security Agreement. The ISA specifies the technical security implementation of the interconnections between two systems. The contents of the ISA must include:

   a. Identification of the MOU associated with the ISA.

   b. Personnel points of contact for both interconnected systems, including the cognizant DAAs.

   c. Identification of the systems being interconnected.

   d. Baseline configuration of the interface (e.g., identification of hardware specifications, identification of protocols, identification of data formats, identification of allowed services).

   e. The security parameters exchanged between the systems to authenticate the legitimacy of the requesting system.

   f. The security controls implemented to protect the confidentiality, integrity, and availability of the connected systems and the information that passes between them.

   g. The services, protocols, software ports, and associated applications and direction of data flow.

TMR-5-3, Interconnection Interface Requirements

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing the policies and requirements for the interconnection interfaces between information systems to be used by all operating units, programs, and systems. These requirements must include the following:

1. Unclassified Information Systems. The controls for interconnecting unclassified information systems are based on each Information System's security category impact levels (see DOE CIO TMR-1).

   a. If the security category impact levels of the information systems are equal, each system's implemented security controls can be relied on to preserve information confidentiality and need-to-know. (Note: Users are still responsible for ensuring that the recipient of information has a need-to-know for the information.).

   b. If the security category impact levels of the information systems are different, a controlled interface is required to adjudicate the differences in security policies and practices.

2. National Security Systems (NSS). The controls for interconnecting National Security System are based on the Protection Index of each information system (see DOE M 205.1-4).

   a. If the Protection Indices of the information systems are equal, each system's implemented security controls can be relied on to preserve information confidentiality and need-to-know of each interconnected system. (Note: Users are still responsible for ensuring that the recipient of information has a need-to-know to include formal access to any Sigma level for the information.)

   b. If the Protection Indices of the information systems are different, a controlled interface is required to adjudicate the differences in security policies and practices.

3. Information systems that process classified information require a controlled interface to interconnect to information systems processing unclassified information.

4. A controlled interface must be used when interconnecting to systems outside of DOE, such as the Internet, public switched networks, Department of Defense, etc.

TMR-5-4, Controlled Interface Functional Requirements

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing controlled interface functions for all operating units, programs, and systems to:

1. Monitor and enforce the protection requirements and adjudicate the differences in security policies between information systems.

2. Prevent unauthorized access to connected systems.

3. Base routing decisions on information that is supplied or alterable only by the controlled interface security controls.

4. Define, document, and implement security controls for the controlled interface (technical, management, operational) for the information type/group with the highest impact or Consequence of Loss of any connected information system. Additional security controls may be added to mitigate any additional risks.

5. Ensure that the interface does not run any user code.

6. Ensure that any possible failures of the controlled interface do not result in loss of confidentiality or unacceptable exposure to loss of integrity or availability.

7. Ensure that communication policies and connections not explicitly permitted in the ISA are prohibited.

8. Ensure that only system administrators, Information System Security Officers, and maintenance staff have interactive access.

9. Prevent unauthorized access to or through the controlled interface or circumvention of the controlled interface from other applications.

10. Isolate the interconnected systems and provides boundary protection services to prevent malicious access and malicious traffic between the interconnected systems.

11. Sample and review all information flowing between the interconnected systems during operation to verify that only authorized information (e.g. messages, files, etc.) is being transmitted. Senior DOE Management must define in the PCSP a graded approach to sampling for information transfer between interconnected systems.

12. Train all users (including privileged users) of the controlled interface in its operation.

13. Ensure that the interconnection of systems does not adversely affect the integrity or availability of the connected systems.

TMR-5-5, Operating Unit Interconnected Systems Management

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