Cyber Security Technical and Management Requirements

Risk Management (TMR-3)
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.

This TMR establishes a structured risk management approach that provides for cost-effective, threat-based implementation and aids Senior DOE Management and operating unit staff in understanding their roles and responsibilities for managing and mitigating risk. It also provides for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology 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-3, *Risk Management Guidance*, dated June 30, 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-3-1, Senior DOE Management Risk Management Program

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing a risk management program for all operating units, programs, and systems. Senior DOE Management must ensure that risk identification and assessment efforts are coordinated and consistent throughout the organization. At a minimum, the Senior DOE Management risk management program is to include the following risk management activities.

1. Risk Assessment. Identify and analyze (quantify) prospective events in terms of probability and consequences/impacts. The following elements are required:

   a. Identify and describe the threats (e.g., DOE Threat Statement, Senior DOE Management defined threats, etc.) used to define the minimum set of controls in the PCSP.
   b. Assess threats, likelihood of adverse actions, and potential consequences.
   c. Quantify the level(s) of risk based on the assessment.
   d. Document the risk determined during the assessment.

2. Risk Mitigation. Use documented findings from the risk assessment as input for the mitigation process. To complete the risk mitigation function, identify minimum security controls by selecting/developing those that provide the greatest level of risk reduction at the lowest cost.

3. Evaluation and Assessment. Evaluate risk reduction achieved and continuously monitor the systems to ensure that security controls are functioning as expected. To accomplish this evaluation and provide appropriate feedback, a process must be implemented to validate the results of risk assessment and mitigation including verification that:

   a. The first two activities (risk assessment and risk mitigation) are properly documented and reflected in the system configuration baseline,
   b. Security controls are implemented,
   c. Risk levels after mitigation are documented as the residual risk, and
   d. Recurring accreditation processes are in place to track the system and schedule appropriate testing and evaluation activities.

TMR-3-2, Risk Management Processes

The Senior DOE Management PCSP is to document risk management processes for all operating units, programs, and systems. At a minimum, the PCSP is to address the processes described below.

1. Develop and implement a risk management approach for unclassified and National Security Systems to provide ongoing assurance that the information systems are operating under approved security controls and that risk is maintained at an acceptable level.

   a. Use the DOE Threat Statement and any Senior DOE Management threat information (as defined in the PCSP) to identify perpetrators and an initial suite of threats. Any organizational, operating unit, and/or system unique threat(s) must be added to that threat suite.

b. Assess the level of risk for each information system by determining the system category as described in DOE CIO TMR-1, *Management, Operational, and Technical Controls*, and DOE M 205.1-4, *National Security System Manual*. Once identified, use the system category to select minimum security controls and perform any adjustments.

c. Document system changes that might require design changes, changes in the systems environment (physical, logical, operational), and newly identified threats that could alter the system's risk profile. Report all such changes to the organization's Designated Approving Authority (DAA).

d. Implement and document prudent risk reduction controls to assure that system security is operating as intended.

2. Develop and implement strong configuration management and security control monitoring to maintain acceptable levels of risk.

3. Identify personnel for the roles and responsibilities in DOE TMR-0, *DOE Cyber Security Program Foundation*, for incorporating risk management concepts and principles into the system and environment.

4. Evaluate each proposed system change(s) to determine if it might introduce a new vulnerability or negate the mitigation of existing risks. If the change(s) impact the risk level accepted by the DAA, it is a security-significant change, and the system must be re-accredited. A control process that evaluates and documents the risk impact incurred by each change and cumulative changes must be implemented.

TMR-3-3, Operating Unit Policies and Procedures

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