

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

**RISK MANAGEMENT
GUIDANCE**



June 30, 2006

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance applies Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for the Security Categorization of Federal Information and Information Systems*, and FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, and implements National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management for Information Technology Systems*, and other applicable Departmental and Federal information technology security laws and regulations.

This Guidance provides additional information for Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls* and DOE CIO Guidance CS-22, *National Security Systems Controls*, in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to the Risk Assessment controls in those documents.

Proper use of the methodology will assure DOE a consistent, standard life cycle approach to managing risks to information and information systems throughout the Department. Senior DOE Management will benefit from the risk management activities performed on their information systems in the following ways:

- Improved understanding of mission risks as they relate to the operation of information systems;
- Clearly defined information system boundaries and interconnection agreements between system boundaries;
- Heightened information security awareness;
- Validated and monitored security controls;
- Measured levels of risk based on identified threats and vulnerabilities; and
- Uniform General Support System (GSS) and Major Application (MA) inventories (i.e., information sensitivity and mission criticality levels)

The DOE CIO will review this Guidance annually and update it as necessary. DOE Senior Management, and their operating units, may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

This Guidance includes a description of the full life cycle, risk management approach that provides for a cost-effective, threat-based implementation process and includes—

- Identifying, assessing, and understanding risk;

- Determining security needs commensurate with level of risk and magnitude of loss that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Agency;
- Implementing policies, procedures, and controls to adequately and cost effectively reduce risks to an acceptable level;
- Formal authorization for operating the system and acceptance of residual risk; and
- Periodically testing and evaluating the effectiveness of security controls and practices.

3. CANCELLATIONS.

None.

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-3 is Applicable.*

Further, 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) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incorporated into contracts..

- 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 PCSPs are to address this Guidance for all systems hosting unclassified information. 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*, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance, Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program, the requirements of the *National Industrial Security*

Program Operating Manual (NISPOM), and DOE M 471.2-2, *Classified Information Systems Security Manual*, for all National Security systems. 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 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management Program Cyber Security Plans (PCSPs) overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot address all of the criteria by the scheduled milestone, DOE expects Senior DOE Management to establish a Plan of Actions and Milestones (POA&Ms) for implementation of this Guidance into their PCSP.

6. CRITERIA.

a. Risk Management.

Risk management is composed of risk assessment, mitigation, and evaluation and continuous assessment. Each requires a cost-effective structured process for identifying, analyzing, and reducing the potential impact of risk events. The structured process helps Senior DOE Management and operating unit staff to understand their roles and responsibilities for managing and containing risks associated with cyber security assets. Risk management is applicable to systems regardless of their stage in the system life cycle.

A uniform risk management process permits managers to—

- Effectively secure DOE general support systems (GSSs) and major applications (MAs),
- Make informed risk management decisions and focus information technology expenditures on mitigating current risk factors,
- Ensure interoperability and portability, and
- Understand total operational and residual risk.

This approach includes—

- Identifying system and environmental threats and vulnerabilities,
- Documenting decisions on the adequacy and maintenance of security controls,

- Determining cost implications of enhanced protection,
- Accepting residual risk, and
- Providing continuous monitoring of the system and environment to ensure that controls are performing as required and changes in network, physical security, and/or operations do not have an adverse impact on the system.

The major activities for conducting a risk management analysis include:

- (1) Risk Assessment. Identify and analyze (quantify) prospective events in terms of probability and consequences/impacts. The following are required elements of risk assessment.
 - (a) Identify and describe each organizational system.
 - (b) Assess threats, vulnerabilities, likelihood of adverse actions, and potential consequences.
 - (c) Quantify the level(s) of risk based on the assessment.
 - (d) Develop a set of security controls based on the level(s) of risk.
 - (e) Document decisions made during the assessment.
- (2) Risk Mitigation. Documented findings from the risk assessment are used as input for the mitigation process. Use the risk assessment to prioritize actions that will most likely result in maximum risk reduction. To complete the risk mitigation function, the following actions are required.
 - (a) Evaluate security controls and select those that provide the greatest level of risk reduction at the lowest cost.
 - (b) Identify appropriate security controls and assign responsibility to those individuals who will implement and maintain those controls.
 - (c) Implement security controls and document the implementation to provide input to the configuration baseline.
- (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 baseline,
 - (b) Security controls are implemented,

- (c) Uncompensated risks are documented as the residual risk
 - (d) Recurring accreditation processes are in place to track the system and schedule appropriate testing and evaluation activities,
 - (e) Employees understand their responsibilities, and
 - (f) Appropriate awareness and training functions are set up properly.
- b. Program Cyber Security Plan. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement a cost-effective, risk-based approach to risk management, including policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.
- (1) Develop and implement a risk management approach, including risk assessments, risk mitigation, residual risk acceptance, and evaluation and continuous assessment, for unclassified and National Security information 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 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. Once identified, use risk levels to select minimum security controls that mitigate risk.
 - (c) For unclassified systems, use the FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, framework for determining Security Categories based on the potential impact of risks to the confidentiality, integrity, and availability security objectives.
 - (2) Develop and implement strong configuration management and system tests and evaluation to maintain acceptable levels of risk, as described in DOE CIO Guidance.
 - (3) Identify personnel for the roles and responsibilities in DOE CIO Guidance CS-2, *Certification and Accreditation Guidance*, for incorporating risk management concepts and principles into the system and environment.

c. Significant Changes.

- (1) A significant change may result from the introduction of new technologies, changes in system configuration, changes in the systems environment (network, physical, operational), operational procedures, or the identification of vulnerabilities (for example, incorporating wireless devices or networks into a wired legacy information system or identifying new vulnerabilities or threats), etc.
- (2) Risk management processes should be in place to evaluate the changes and determine if the change has introduced a new vulnerability or threat or negated the mitigation of existing threats. If the change has increased the risk to an unacceptable level it is considered a significant change.
- (3) When a significant change occurs, the risk assessment should be reviewed and updated as needed. System Security Plans must also be updated to reflect any changes to the level of risk and the related risk mitigation controls, techniques, and methods used. If the level of risk is increased by a significant change, existing authorizations to process for that system or application (accreditation) are invalidated and re-authorizations must be sought.
- (4) As described in DOE CIO Guidance CS-2, *Certification and Accreditation Guidance*, a management official must authorize, in writing, the use of a system based on implementation of its System Security Plan before beginning operations or when a significant change occurs.
- (5) Owners and operators of interconnected applications and systems must be notified of significant changes to evaluate impacts to their interconnection agreements. Threat statements, system risk assessments, and mitigation plans must be reviewed and updated, as necessary, before incorporating new technology or operational procedures into an approved system boundary.

7. ADDITIONAL CRITERIA FOR NATIONAL SECURITY SYSTEMS.

National Security systems are to be protected according to guidelines of the *NISPOM* and DOE CIO Guidance.

- a. Develop and maintain a System Security Plan that is coordinates with the Site Security Plan and/or Site Safeguards and Security Plan. These documents establish the base level of security required before system development begins or when changes are made to the system. Additionally:
 - (1) Utilize the DOE Threat Statement to identify baseline threats.
 - (2) Utilize the DOE Risk Assessment to identify uncompensated risk.

- (3) Utilize DOE CIO Guidance to identify the Minimum Security Criteria.
- (4) Identify and define threats and their characteristics not included in the DOE Threat Statement.
- (5) Perform a risk assessment for these newly identified threats.
- (6) Document system changes that might require design changes, changes in the systems environment, and newly identified threats that could alter the system's risk profile. Report all such changes to the organization's Designated Approving Authority.
- (7) Implement and document prudent risk reduction controls to assure that the National Security system is operating as intended.

8. RESPONSIBILITIES.

a. Senior DOE Management.

- (1) Assume accountability for risk management and accept overall residual risk throughout their organizations.
- (2) Coordinate the development and implementation of the risk management process, via their PCSPs.
- (3) Designate, in writing, single points of contact to represent their organizations on risk management issues and to whom day-to-day risk management activities may be delegated. NOTE: While authority for ensuring the risk management process may be delegated, accountability remains with Senior DOE Management.
- (4) Ensure that risk for National Security systems under their control are maintained at an acceptable level.

9. REFERENCES.

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

10. DEFINITIONS.

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

11. 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-3 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 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
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration