U.S. Department of Energy
Washington, D.C.

POLICY

DOE P 205.1

5-8-01

SUBJECT: DEPARTMENTAL CYBER SECURITY MANAGEMENT POLICY

PURPOSE AND SCOPE

The Departmental Cyber Security Management (DCSM) Policy was developed to further clarify and support the elements of the Integrated Safeguards and Security Management (ISSM) Policy regarding cyber security. It parallels the ISSM policy and structure, and provides more details to support the implementation within the cyber security realm. The DCSM provides a formal, organized risk management process whereby people plan, perform, assess, and implement processes and controls to ensure the appropriate protection of classified and unclassified information stored, processed, or transmitted on electronic systems. The DCSM is institutionalized through Department of Energy (DOE)/National Nuclear Security Administration (NNSA) directives and contracts to establish the Department-wide cyber security management objectives, fundamentals, and activities.

The contents directly link to all levels of activities and documentation related to cyber security management throughout the DOE/NNSA complex.

Throughout this policy statement, the term cyber security is used to mean the physical, technical, and administrative controls and risk management processes for providing the required and appropriate level of confidentiality, integrity, availability and accountability for DOE/NNSA information stored, processed, or transmitted on electronic systems (and networks).

POLICY

The Department is committed to conducting work efficiently and securely, and in a manner that ensures the appropriate protection of classified and unclassified information controlled on electronic systems through risk management. It is Department policy that cyber security management described herein be used to systematically integrate cyber security into management and work practices at all levels so that missions are accomplished while appropriately protecting electronic information and electronic information systems.

Like the ISSM Policy, the DCSM establishes a hierarchy of elements to facilitate the orderly development and implementation of cyber security management throughout the DOE/NNSA complex. Cyber security management consists of six elements: (1) objectives, (2) guiding principles, (3) core functions, (4) mechanisms, (5) responsibilities, and (6) implementation.

The objectives, guiding principles, and core functions of cyber security management identified below must be used to consistently implement cyber security management throughout the DOE/NNSA complex. The mechanisms, responsibilities, and implementation components are established for all electronic systems and will vary based on specific risk assessments, which will include any specific threats, vulnerabilities, and criticality of the electronic information, electronic information systems, and missions they support.

Component 1 - Objectives of the DCSM

The Department and its contractors must systematically integrate cyber security into management and work practices at all levels so that missions are accomplished while protecting electronic information and electronic information systems. This is to be accomplished through effective integration of cyber security management into all facets of work planning and execution. In other words, the overall management of cyber security functions and activities becomes an integral part of mission accomplishment.

Component 2 – Guiding Principles

The guiding principles are the fundamental policies that guide Department and contractor actions, from the development of cyber security directives to the performance of work.

Individual Responsibility and Participation. Each individual is directly responsible for protecting information within his or her span of control. Information controlled on electronic systems is an essential DOE/NNSA asset and thus requires protection according to its importance to the missions of the Department.

Line Management Responsibility for Cyber Security. Cyber security is a key business function; the decision to operate an electronic information system with appropriate protection measures is a line management responsibility. Appropriate risk analysis is performed prior to work being authorized. Residual risk must be accepted by line management and controls must be in place and verified prior to authorization of operations.

Clear Roles and Responsibilities. Clear and unambiguous lines of authority and responsibility for ensuring cyber security will be established and maintained at all organizational levels within the Department and its contractor organizations.

Competence Commensurate with Responsibilities. Personnel must possess the experience, knowledge, skills, and abilities that are necessary to discharge their responsibilities. Cyber security awareness, training, and education are key to providing the knowledge, skills, and abilities required.

Balanced Priorities. Cyber security controls are tailored to risks. Resources must be effectively allocated to address cyber security and operational considerations. Protecting DOE/NNSA electronic information resources must be a priority whenever activities are planned and performed. The implementation of security should be based on cost-effective controls commensurate with the risk.

Identification of Safeguards and Security Standards and Requirements. A structured risk management process can be used to establish priorities and information sharing can be used to optimize balance within safeguards and security. Managing cyber security risks is a process of identifying and assessing threats, vulnerabilities, asset value, and existing protection measures; developing and implementing appropriate policies and controls; promoting awareness of those policies and controls; and monitoring, evaluating, and improving the effectiveness of policies and controls. These risk assessments will be combined with existing risk assessments for non-electronic forms of information to provide a complete picture of risks and protection needs for our information.

Tailoring of Protection Strategies to Work Being Performed. A performance-based approach, with appropriate measures of effectiveness and performance, supports the tailoring of protection strategies, helps to document improvements, and guides further progress.

Component 3 – Core Functions

These five core cyber security management functions (paralleling those from the ISSM Policy) provide the necessary structure for any mission activity that generates, uses, stores, transmits, or processes information on Departmental electronic systems. The functions are applied as a continuous cycle with the degree of rigor appropriate to address the type of mission activity and the risks involved. The Office of the Chief Information Officer, a central focal point to oversee the cyber security management, provides cyber security policy, coordination, and assessment in support of line organizations.

Define the Scope of Work. Identify information assets on electronic systems and their criticality to the organization's mission. Programmatic missions are accomplished through the effective use of information assets on electronic systems. These assets may be critical to specific programmatic missions or provide support for other programmatic missions.

Analyze the Risk. Through the risk management process, risks to information assets on electronic systems are identified, analyzed, and categorized. These risk assessments are based on the correlation of specific threats and vulnerabilities with asset value and protection measures.

Develop and Implement Security Measures. Risk management is used to determine appropriate business or residual risks to the confidentiality, integrity, and availability of information assets on electronic systems. Applicable technical, physical, and administrative controls to reduce or mitigate risks are identified, agreed upon, and implemented. Line management accepts the residual risk through the implementation of appropriate protection measures and strategies.

Perform Work Within Measures and Controls. Ensure that information on electronic systems and electronic information systems is protected in accordance with the risks and security measures implemented.

Provide Feedback and Continuous Improvement. Monitor and evaluate the effectiveness of the DCSM. Feedback information (performance measures and testing) on the adequacy of cyber security is gathered, opportunities for improving cyber security effectiveness are identified and implemented, line and independent oversight is conducted, and, if necessary, enforcement actions occur. Sharing successes and lessons learned is key to implementing successful risk management programs consistently across a variety of DOE/NNSA organizations.

Awareness is promoted throughout the organization. Users are continually educated to understand the risks (threats and vulnerabilities) and provided the skills to practice the related procedures and controls to mitigate the risks that are under their control.

Component 4 - Mechanisms

Cyber security mechanisms are established by senior departmental management in collaboration with the CIO and are expressed through directives (Policy, Rules, Orders, Notices, Standards, and guidance) and contract clauses.

Component 5 - Responsibilities

Responsibilities must be clearly defined in documents appropriate to the activity or mission. DOE/NNSA responsibilities are defined in Department directives. Contractor responsibilities are detailed in contracts, regulations, and contractor-specific procedures. For each management mechanism employed to satisfy a cyber security management principle or function, the associated approval authority needs to be established. The review and approval levels may vary commensurate with the type of electronic information assets and risks involved.

Component 6 - Implementation

> Cyber security implementation describes how the core cyber security functions are performed. Implementation may vary from facility to facility and from activity to activity and involve specific instances of mission, purpose, electronic information asset identification, threat and vulnerability identification and analysis, definition and implementation of protective measures and controls, life-cycle management, and monitoring and assessing cyber security performance for improvement.

Contractor policies, procedures, and documents (e.g., Cyber Security Program Plans, Training and Awareness Plans, System Security Plans) are established to implement the various aspects of cyber security management and fulfill commitments made to the Department.

SPENCER ABRAHAM
Secretary of Energy