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

POLICY

DOE P 470.1

Approved: 5-8-01

SUBJECT: INTEGRATED SAFEGUARDS AND SECURITY MANAGEMENT (ISSM) POLICY

PURPOSE AND SCOPE

Safeguards and security management systems provide a formal, organized process for planning, performing, assessing, and improving the secure conduct of work in accordance with risk-based protection strategies. These systems are institutionalized through Department of Energy (DOE) directives and contracts. The purpose of this Policy is to formalize an Integrated Safeguards and Security Management (ISSM) framework.

The ISSM system framework encompasses all levels of activities and documentation related to Safeguards and Security management throughout the DOE complex.

Throughout this Policy statement, the term ISSM includes all topical areas of safeguards and security (e.g., personnel, physical, information, nuclear safeguards, cyber security) and related cross-cutting areas (e.g., export control, classification, foreign visits and assignments, and foreign travel). ISSM will ensure the adequate protection of DOE assets (e.g., classified matter, unclassified sensitive matter, and Government property).

POLICY

The Department is committed to conducting work efficiently and securely. It is Department policy that the ISSM framework shall be used to systematically integrate safeguards and security into management and work practices at all levels so that missions are accomplished securely. Direct involvement of all personnel during the development and implementation of an ISSM framework is essential for success. The ISSM framework will be implemented through programmatic directives and other related directives (see references).

The ISSM framework establishes a hierarchy of components (see figure 1). To facilitate the orderly development and implementation of safeguards and security management throughout the DOE complex, the ISSM framework consists of six components:

1. the objective,
2. guiding principles,
3. core functions,
4. mechanisms,
5. responsibilities, and
6. implementation.

The objective, guiding principles, and core functions of ISSM identified below must be used consistently throughout the DOE complex. The mechanisms, responsibilities, and implementation components are established by sites for all work.

COMPONENT 1: Objective of Integrated Safeguards and Security Management

Perform Work Securely. The ISSM framework will systematically integrate safeguards and security into management and work practices at all levels so that missions are accomplished securely.

COMPONENT 2: Guiding Principles for Integrated Safeguards and Security Management

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

Individual Responsibility and Participation. Each individual is directly responsible for following security requirements and contributing to secure missions and workplaces.

Line Management Responsibility for Safeguards and Security. Line management is directly responsible for the protection of the DOE assets. 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 safeguards and security must be established and maintained at all organizational levels within the Department and its contractors.

Competence Commensurate with Responsibilities. Individuals must possess the experience, knowledge, skills, and abilities necessary to fulfill their responsibilities.

Balanced Priorities. Resources must be effectively allocated to address safeguards and security, programmatic, and operational considerations, realizing that achieving programmatic goals is a significant component of achieving safeguards and security. Protecting the DOE assets must be a priority whenever activities are planned and performed.

Identification of Safeguards and Security Standards and Requirements. Before work is performed, the associated risk must be evaluated, and an agreed-upon set of safeguards and security standards and requirements shall be established that, if properly

implemented, will provide appropriate assurance that DOE assets, the worker, the public, and the environment are protected from adverse consequences.

Tailoring of Protection Strategies to Work Being Performed. Administrative and engineering controls to prevent and mitigate risk must be tailored to the work being performed.

COMPONENT 3: Core Functions for Integrated Safeguards and Security Management

These five core ISSM functions provide the necessary structure for any work activity. The functions are applied as a continuous cycle with the degree of rigor appropriate to address the type of work activity and the risk involved.

Define the Scope of Work. Missions are translated into work, potential requirements identified, expectations set, tasks identified and prioritized, related security assets identified, and resources allocated.

Analyze the Risk. Risks associated with the work are analyzed to determine applicable requirements.

Develop and Implement Security Measures. Measures and controls are tailored and implemented to mitigate risk. Residual risk is accepted by line management.

Perform Work within Measures and Controls. Authorized security measures are in place and work is performed accordingly.

Provide Feedback and Continuous Improvement. Feedback information on the adequacy of measures and controls is gathered. Opportunities for improving the definition and planning of work are identified and implemented. Best practices and lessons learned are shared.

COMPONENT 4: Mechanisms for Integrated Safeguards and Security Management

ISSM mechanisms are the information and tools used to implement the guiding principles and core functions. They may vary between facilities and activities based on the risk and the work being performed.

COMPONENT 5: Responsibilities for Integrated Safeguards and Security Management

Responsibilities must be clearly defined in documents appropriate to the activity. DOE responsibilities are defined in Department directives. Contractor responsibilities are detailed in contracts, regulations, and contractor-specific procedures. Review and approval levels may vary, commensurate with the type of work and risk involved.

COMPONENT 6: Implementation of Integrated Safeguards and Security Management

Implementation involves integrating specific instances of defining and planning work, formally identifying and analyzing risk, developing and implementing measures and controls, performing work, and monitoring and assessing performance for feedback and improvement.

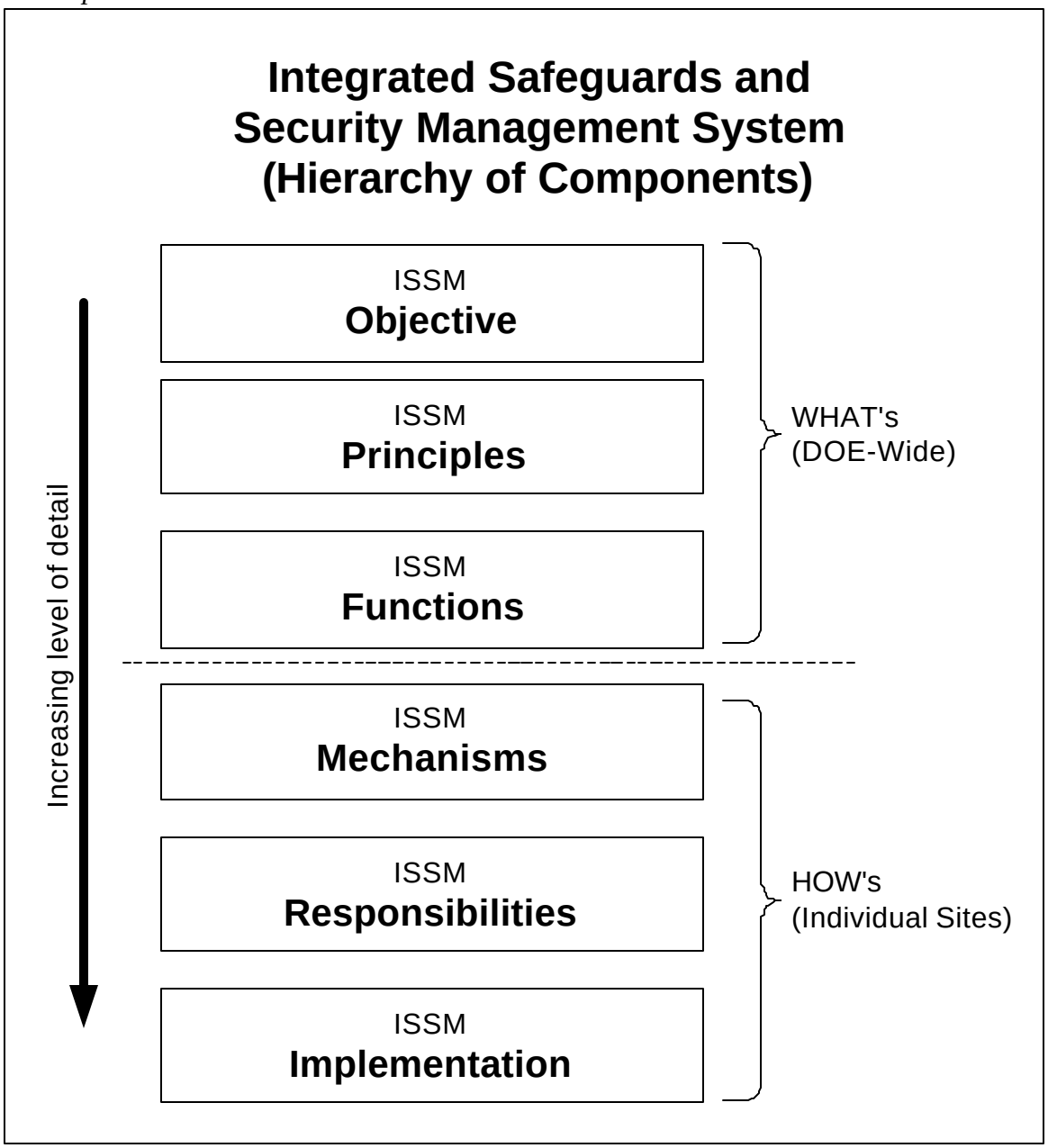

Figure 1.

APPLICABILITY

DOE Elements. This Policy applies to all DOE elements, including the National Nuclear Security Administration.

Deputy Administrator for Naval Reactors. Due to the dual-agency (Navy/DOE) nature of the Naval Nuclear Propulsion Program as described in Executive Order 12344 (set forth in Public Law 106-65), the Deputy Administrator for Naval Reactors will implement this Notice as appropriate for Naval Nuclear Propulsion Program employees.

REFERENCES

- DOE P 142.1, *Unclassified Foreign Visits and Assignments,* dated 7-14-99.
- DOE N 142.1, *Unclassified Foreign Visits and Assignments*, dated 7-14-99.
- DOE N 470.2, *Unofficial Foreign Travel,* dated 12-15-00.
- DOE O 551.1A, *Official Foreign Travel,* dated 8-25-00.
- DOE M 475.1-1, *Identifying Classified Information,* dated 5-8-98.
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information,* dated 6-30-00.
- DOE M 471.1-1, *Identification and Protection of Unclassified Nuclear Information Manual,* dated 6-30-00.
- DOE 470.1, *Safeguards and Security Program,* dated 9-28-95.
- DOE P 205.1, *Departmental Cyber Security Management Policy,* dated 5-8-01.

SPENCER ABRAHAM
Secretary of Energy