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

ORDER

DOE O 205.1B

Approved: 5-16-2011

SUBJECT: DEPARTMENT OF ENERGY CYBER SECURITY PROGRAM

1. PURPOSE. To set forth requirements and responsibilities for a Departmental Cyber Security Program (CSP) that protects information and information systems for the Department of Energy (DOE). The CSP requires a Risk Management Approach (RMA) that includes: analysis of threats/risks; risk-based decisions considering security, cost and mission effectiveness; and implementation consistent with guidelines from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) cyber requirements, processes and protections. *DOE Oversight* is conducted through *Assurance Systems* that monitor the risk evaluation and protection processes at each level in the organization. The DOE CSP emphasizes risk management rather than a systems-level "controls compliance" approach. Through the RMA, the Department effectively and efficiently meets its obligations under the Federal Information Security Management Act (FISMA) in a manner that improves, rather than impedes the fulfillment of the Department's statutory missions.

   The CSP, through DOE's RMA:

   a. establishes line management accountability for ensuring protection of information and information systems through Senior DOE Management (SDM) consisting of the Department's Under Secretaries, the Energy Information Administrator, Power Marketing Administrators and the Chief Information Officer (CIO) (see *Attachment 3* for a pictorial representation of DOE SDM;

   b. recognizes the Department's federated government-owned/contractor operated (GOCO) environment and appropriately integrates cyber security governance, accountability and reporting into management and work practices at all levels of the Department;

   c. institutes a mission-centric, risk-based approach to the management of cyber security to ensure the confidentiality, integrity, and availability of DOE information and information systems;

   d. requires a training, education, and awareness program that develops and maintains cyber security competencies including threat identification and risk management throughout DOE Federal and contractor workforces that enables personnel to fulfill their responsibilities in protecting DOE information and information systems;

   e. establishes cyber security governance processes that are mission-focused;

   f. defines enterprise-level cyber security requirements, processes and responsibilities for protecting unclassified and national security information and information systems; and

g. ensures that the focus of cyber protection is on accomplishing mission, threat response, and affordable risk mitigation strategy that provides the appropriate benefit from available cyber security resources.

2. CANCELLATION.

a. DOE O 205.1A, *Department of Energy Cyber Security Management Program*, dated 12-4-06.

b. DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

c. DOE M 205.1-5, *Cyber Security Process Requirements Manual*, dated 8-12-08.

d. DOE M 205.1-6, *Media Sanitization Manual*, dated 12-23-08.

e. DOE M 205.1-7, *Security Controls for Unclassified Information Systems Manual*, dated 1-5-09.

f. DOE M 205.1-8, *Cyber Security Incident Management Manual*, dated 1-8-09.

Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

a. Departmental Elements. Except for the equivalencies/exemptions in paragraph 3.c, this directive applies to all Departmental elements.

The Administrator of NNSA will assure that NNSA employees and contractors comply with their respective responsibilities under this directive. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

The Administrator of Bonneville Power Administration (BPA) will assure that BPA employees and contractors comply with their respective responsibilities under this directive.

For the purposes of this Order, the following Departmental Elements are identified as SDM and are responsible for formally implementing the DOE RMA described in this Order:

(1) The Office of the Under Secretary of Energy

(2) The Office for the Under Secretary of Science

(3) The National Nuclear Security Administration (NNSA)

(4) Energy Information Administration (EIA)

(5) Bonneville Power Administration (BPA)

(6) Southeastern Power Administration (SEPA)

(7) Southwestern Power Administration (SWPA)

(8) Western Area Power Administration (WAPA)

(9) The Office of the Chief Information Officer (OCIO)

(10) The Office of the Under Secretary for Nuclear Security (other than NNSA)

b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c. the Contractor Requirements Document (CRD) sets forth requirements of this Order that will apply to contracts that include the CRD.

(1) The CRD, *Attachment 1*, sets forth requirements of this directive that will apply to site/facility management and operating (M&O) contracts that include the CRD.

(2) A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data (RD) or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, —Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.

c. Equivalencies/Exemptions for DOE O 205.1B. Requests for equivalencies and exemptions from paragraph 4, of this Order must follow the process outlined in paragraph 6.a.(3) (c) of DOE O 251.1C. Request for equivalencies or exemptions from subsequent implementation plan requirements established by SDM must be addressed as prescribed in such plans.

Exemption. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Order for activities under the Deputy Administrator's cognizance, as deemed appropriate.

4. REQUIREMENTS. The DOE RMA employs an integrated enterprise-wide approach to secure information and information systems. Managing information security risk, as risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations—providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of those organizations. The DOE RMA provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by NIST security standards and guidelines, operational awareness, and site expertise.

DOE information and information systems must be protected in a manner commensurate with impact to mission, national security, risk, and magnitude of harm.

a. Governance.

(1) The CSP and DOE RMA are governed by the Department's Information Management Governance Council (IMGC). The IMGC serves as the DOE corporate risk executive (function).

(a) The DOE Under Secretaries, NNSA Administrator and the DOE CIO are the full, voting members of the IMGC.

(b) The Chief Health, Safety and Security Officer and the Director, Office of Intelligence and Counterintelligence are advisory, non-voting members of the IMGC.

(2) The IMGC is supported by:

(a) Information Management Governance Council Representatives (IMGCR), consisting of one Federal representative each from the Office of the Under Secretary of Energy; the Office of Science; the NNSA; and the Office of the CIO.

(b) Information Management Governance Council Advisory Group (IMGCAG), consisting of: four members selected by the M&O community and approved by the IMGC: one CIO selected from the National Laboratories reporting to the Office of the Under Secretary of Energy; one CIO selected from the National

Laboratories reporting to the Office of Science; one CIO selected from the National Laboratories reporting to NNSA; and one CIO selected from the NNSA production facilities reporting to NNSA.

(c) Information Management Governance Secretariat, provided by the DOE Office of the CIO to manage the administrative functions of the IMGC.

b. The RMA Process.

(1) The RMA is applicable to the management of all information and information systems.

(2) At all levels of DOE, the RMA must implement the four components of risk management: framing; assessing; responding; and monitoring as depicted in *Figure 1*.

(a) Risk framing (Step 1) and the risk assessment (Step 2) are completed in partnership with the *DOE Oversight* function.

(b) Risk response (Step 3) ensures the defensive protections are adequate for the agreed upon risk profile. For example, at the DOE Site level, the Senior Contractor Site Manager is accountable (e.g. Laboratory Director, Plant Director) for ensuring the defensive protections are adequate to mitigate the risk profile agreed to by the Federal Site Manager and Senior Site Manager.

(c) The site is responsible for developing an ongoing monitoring approach to evaluate and respond to changes in the environment and assess overall performance (Step 4). *DOE Oversight* is a component of risk monitoring and is accomplished through review of risk assessments, *Assurance System* outputs and processes, as appropriate.

(3) SDM shall establish the organizational tolerance for risk and communicates the risk tolerance throughout the organization including guidance on how risk tolerance influences ongoing decision-making activities.

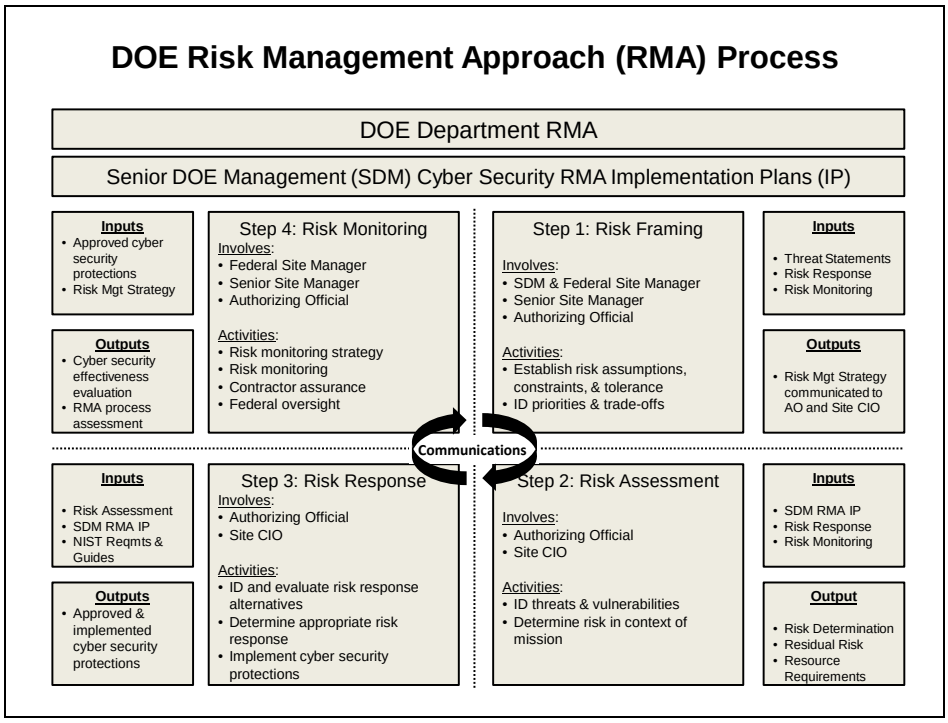


Figure 1. DOE Risk Management Approach (The 4-Steps are displayed at the DOE Site Level as an example)

(4) SDM must, using a risk based and tailored approach, flow down the requirements and responsibilities of this Order to all subordinate organizational levels through implementation plans.

(5) The development of SDM RMA implementation plans must be coordinated with the DOE CIO, and with the IMGC to resolve cross-SDM issues.

(6) Authorization Function -- the Authorizing Official (AO) is the Federal official(s) responsible and accountable for ensuring that information systems under their purview are operated at an acceptable level of risk:

(a) For NSS, the Federal AO function is accomplished through *DOE Oversight* and must be consistent with CNSS policy.

(b) For unclassified systems, the Federal AO function is accomplished through *DOE Oversight*, which includes *Assurance System* transparency and performance according to the site's risk management plan, not necessarily a "system by system" authorization action.

c. SDM Risk Management Implementation Plans.

(1) Must be based upon requirements, guidance and processes of applicable NIST and CNSS publications, as well as other appropriate national standards, whether or not specifically stipulated in this Order.

(2) Must provide the framework for establishing acceptable risk in context of mission performance and assurance.

(3) Must utilize a partnership approach that includes the Federal Site Manager and consultations with the Senior Site Manager in establishing acceptable risks.

(4) Must provide sufficient flexibility in the design of organizational and site RMA implementation plans such that sites can tailor cyber security protections based on risk assessments to cost-effectively reduce information security risks to an acceptable level, including the tailoring of the requirements below.

(5) Must focus on oversight of high-level balanced outcomes and the outputs of the *Assurance System* or equivalent.

(6) Must provide a methodology for graded oversight that is based on risk and the contractor's past performance in risk management and tailored to meet mission needs.

(7) Must define (or define processes for developing) minimum required components of applicable assurance systems, such as risk tolerance, and/or performance indicators, objectives, measures, other criteria.

(8) Must define processes, including AO coordination with applicable contracting officials, to evaluate contractor programs, management, and assurance systems, for effectiveness of performance, consistent with DOE Order 226.1A, *Implementation of Department of Energy Oversight Polic*y.

(9) Must require that where mission appropriate, or where DOE Federal or DOE to citizen services are provided, federally directed security initiatives such as Trusted Internet Connection (TIC), Internet Protocol (IP) v6, Domain Name System Security Extensions (DNSSEC) be implemented as part of system development life cycle plans.

(10) Must incorporate requirements for tracking cyber security weaknesses identified for NSS and unclassified information systems in a plan of action and milestone process.

(11) Must require DOE and NNSA NSS and Federal unclassified systems to display a system use notification (e.g. Warning Banner) at login and require users to electronically acknowledge the warning (such as clicking on "OK" or "I agree" button to proceed). An example of a DOE approved warning banner:

****WARNING**WARNING**WARNING**WARNING****

This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities.

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.
****WARNING**WARNING**WARNING**WARNING****

(12) Must address risk-based protection of information on media used by or produced by NSS and unclassified information systems.

(13) Must define a process for incident reporting that requires all cyber security incidents involving information or information systems, including privacy breaches, under DOE or DOE contractor control must be identified, mitigated, categorized, and reported to the Joint Cybersecurity Coordination Center (JC3) in accordance with JC3 procedures and guidance. JC3 procedures will incorporate reporting requirements from OMB and the Department of Homeland Security and be consistent with classified information and incident handling procedures in Department directives. If loss or unauthorized disclosure of classified information associated with NSS is suspected, the incident must be immediately reported to the AO.

(14) Must require appropriate controlled unclassified information marking in the electronic environment. The requirements of DOE

M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*, and DOE Order 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information* must be implemented for all DOE and NNSA information and information systems.

(15) Must require appropriate classification marking in the electronic environment. The following must be implemented for all DOE and NNSA NSS. For systems with Restricted Data (RD), Formerly Restricted Data (FRD) or Transclassified Foreign Nuclear Information (TFNI), implementation should be consistent with DOE M 470.4-4A, *Information Security Manual* or NAP 70.4, *Information Security for NNSA*, and DOE O 475.2A, *Identifying Classified Information*. For systems with National Security Information, implementation must be consistent with DOE M 470.4-4A, DOE O 475.2A, and 32 CFR 2001.23.

(16) Must require that National Security Systems follow CNSS. The security and risk management of DOE and NNSA systems containing national security information must adhere to the requirements established by the CNSS. Requests for equivalencies and for exemptions from CNSS requirements must follow those processes, as amplified by SDM cyber security implementation plan direction.

(17) Must address requirements for information and communications technology (ICT) supply chain risk management (SCRM) as part of the RMA. Requirements must be consistent with NIST guidance, CNSS requirements, and other Departmental Directives. Additional information concerning ICT SCRM considerations is delineated in Appendix A.

(18) Must require appropriate media sanitization for NSS.

(a) Electronic media that is utilized on NSS must be sanitized prior to disposal according to DOE and NNSA media sanitization requirements documented by the AO approved processes in the SDM RMA implementation plan.

(b) Disposal of NSS electronic media must be consistent with DOE and NNSA record retention schedules and requirements.

(19) Must use the information types and their indicated hierarchical protection levels to guide risk-based decisions in the implementation of the RMA. For classified systems the AO establishes, based on risk acceptance, the appropriate level of

controls required to authorize use of these systems. Table 1 maps the information classification levels from Executive Order (E.O.) 13526 and 10 CFR part 1045 (Confidential, Secret and Top Secret) to the CNSSI 1253 potential impacts of Low, Moderate and High.

TABLE 1. MAPPING DOE Information Groups to CNSSI 1253 Potential Impact Levels

DOE Information Group [1]			CNSSI 1253 Potential Impact for Loss of Confidentiality
Confidential (NSI)			Low
Confidential RD[2] [4]			Moderate
Confidential RD[2][4]	Sigma	1, 2, 3, 4, 5, 9, 10, 11, 12, and 13	Moderate
Secret (NSI)			Moderate
Secret RD			Moderate to High
Secret RD [3]	Sigma	1, 2, 3, 4, 5, 9, 10, 11, 12, 13, 15 and 20	Moderate to High
Secret RD [3]	Sigma	14	High
Top Secret (NSI) Top Secret RD			High

[1] Potential levels of impact for Integrity and Availability are determined by use of the data as specified by the Information and Information System Owner as part of the Information System Categorization process of CNSSI 1253.
[2] RD is governed by the Atomic Energy Act of 1954 and requires additional access authorization. Consequences from unauthorized disclosure can be more severe than for the commensurate level of National Security Information (NSI). The RD category has no automatic "Declassify On: (date or event)" as does NSI.
[3] Secret RD and Secret RD with Sigmas start at the highest CNSSI 1253 Potential impact for Loss of Confidentiality using the Risk Management Approach to make decisions to reduce controls.
[4] CRD is moderate impact.

(20) Must include requirements for protecting RD, FRD and TFNI on NSS consistent with DOE O 5610.2 Chg 1, *Control of Weapon Data*. When RD, FRD, or TFNI is provided to personnel from other Government Agencies, the RMA implementation plans must ensure that such personnel follow the requirements contained in this Order.

(a) Electronic Transmission. Non-Sigma Nuclear Weapons Data (NWD) must be sent electronically only over approved classified networks and only if need-to-know for that information is assured by the sender.

i. Non-Sigma Secret RD NWD may be sent to Department of Defense (DOD) and Other Government Agencies on Secret

Internet Protocol Router Network (SIPRNET) without secondary encryption.

ii. Non-Sigma Secret RD NWD may be sent via DOE Enterprise Secure Network (ESN)
.

(b) Secure Telecommunication Transmission of Non-Sigma NWD using point-to-point secure communication via appropriately certified secure telecommunication systems is permitted at both Secret and Top Secret levels, provided they are consistent with approved site security plans. Access authorization and need-to-know must be verified prior to transmission.

(c) Access Requirements. The access requirements from DOE M 470.4-5, *Personnel Security*, must be implemented for all DOE and NNSA NSS, where RD, FRD or TFNI is stored, processed, or transmitted.

(d) Restricted Data Specific Controls. RD specific controls must be implemented according to DOE M 470.4.4A *Information Security Manual*.

d. Power Marketing Administrations (PMA). At a minimum, PMA protections must comply with North American Electric Reliability Corporation (NERC) standards.

e. Existing authorized systems retain authorization to operate until reauthorization is required, either because the systems have passed the authorization expiration date or because of significant security changes in the security requirements of the information system. Reauthorization must be in accordance with the applicable SDM RMA implementation plan.

5. RESPONSIBILITIES.

a. DOE Under Secretaries, NNSA Administrator.

(1) Serve as a member of the IMGC.

(2) Serve as SDM.

b. Senior DOE Management (SDM). Provide assurance the Department is achieving its missions effectively and efficiently with reasonable risk.

(1) Codify acceptable residual risk, balancing mission performance with cost and risk. Communicate acceptable mission risk to Federal Site Management and Contracting Officers.

(2) Flow down the requirements and responsibilities of this Order to all subordinate organizational levels through implementation plans.

(3) Ensure the preparation and maintenance of organizational RMAs as described in paragraph 4.

(4) Coordinate with the DOE CIO in the development of implementation plans, and with the IMGC to resolve cross-SDM issues.

(5) Serve as the Authorizing Official (AO) for information systems under their purview. This authority may be further delegated within the organization. The delegating official remains responsible and accountable.

(6) Retain overall responsibility and accountability for the RMA within their organization.

(7) Establish and implement an effective oversight program consistent with requirements defined in DOE O 226.1A.

(8) Notify contracting officers of which contracts must incorporate the CRD.

c. Information Management Governance Council (IMGC).

(1) Oversee the CIO's development and management of the CSP, including strategy, the RMA, the Federal security architecture and cyber security incident management.

(2) Ensure the DOE CSP and RMA are aligned with mission requirements and DOE management principles.

(3) Guide DOE efforts in applying Federal standards and requirements related to information management, including determination, in consultation with OMB and relevant interagency stakeholders, of the extent to which new federal requirements/OMB guidance/data calls/etc. would be applied to DOE contractors.

(4) Address broad issues of information management in the Department, as appropriate.

(5) Identify individuals to serve as IMGC Representatives (one Federal representative per IMGC member).

d. DOE Chief Information Officer (CIO).

(1) Fulfill CIO responsibilities as required by the Federal Information Security Management Act of 2002 (FISMA) and related cyber security regulations including:

(a) Serving as the DOE Office of Primary Interest (OPI) for developing and maintaining the Department RMA, cyber security directives, and Departmental cyber threat statement.

(b) Ensuring that cyber security training, education, and awareness that supports role-based competencies is available for the Federal workforce.

(c) Reporting annually to the Secretary, in coordination with the Information Management Governance Council (IMGC), on the effectiveness of the CSP.

(2) Serve as a member of the IMGC.

(3) Serve as SDM for DOE staff and support offices and for Federal information systems. This authority may be further delegated.

(4) Serve as AO for DOE Federal information systems. This authority may be further delegated. The delegating official remains responsible and accountable.

(5) Recommend to the Secretary an individual to serve as the Chief Information Security Officer (CISO) whose responsibilities are defined in FISMA and in paragraph 5.e.

(6) Ensure the Federal cyber security architecture framework supports and enables the Department's missions.

(7) Ensure the integration of cyber security into Departmental Capital Planning and Investment Control (CPIC) processes for Federal investments.

(8) Ensure the requirements established by the Office of Management and Budget (OMB) or other Federal Agencies and Organizations with directive authority in cyber security are coordinated and implemented for information systems operated by or in direct support of Department Program, Staff and Federal Site Offices.

e. Chief Information Security Officer (CISO).

(1) Carry out the responsibilities of the CISO as defined by FISMA.

(2) On behalf of the IMGC and CIO, develop and maintain the Departmental RMA including:

(a) Preparing supplemental implementing guidance as required;

(b) Developing the DOE cyber security threat statement in coordination and consultation with the Office of Intelligence and Counterintelligence;

(c) Coordinating, implementing, and managing a Department-wide cyber security incident reporting, assessment, and response program, including the JC3; and

(d) Directing cyber security incident management in coordination with other Departmental Elements, and other U.S. Government organizations as circumstances warrant, consistent with the standards and guidelines issued by the Department of Homeland Security (DHS).

(3) Coordinate and provide the Department's response for all agency-level cyber security inquiries, FISMA reporting, and CSP review requirements, e.g., Congressional, DHS, and OMB.

(4) Serve as the subject matter expert point of contact for the CIO with the SDM and other Federal agencies regarding cyber security activities.

(5) Coordinate the sharing of threat information with SDMs, the Office of Intelligence and Counterintelligence, and other U.S. Government officials.

(6) Serve as the Agency lead for ICT SCRM, to include, at a minimum, the following enterprise-level functions:.

(a) Establish DOE ICT SCRM policy and develop related guidance as appropriate.

(b) Provide advice and assistance, as necessary, to SDM organizations on matters involving the prevention, detection, and reporting of ICT supply chain issues. Advice and assistance will include, but not be limited to:

1 Product and supplier evaluation

2 Quality control, and configuration and security management

3 Asset management

4 Critical Infrastructure Information (CII) accountability, control, visibility, and protection

5 Weakness/deficiency detection, reduction, and mitigation strategies

6 Incident management

7 Training and awareness

8 Monitoring and reporting

(c) Provide data analysis and support services, as required.

(d) Monitor, review, and assess the effectiveness of enterprise ICT SCRM processes.

f. Information Management Governance Council Representatives (IMGCR).

(1) Serve as subject matter expert staff for the IMGC and support activities necessary for DOE CSP development and implementation.

(2) Provide input and recommendations for new or revised cyber security policy.

(3) Provide recommendations to the IMGC on the applicability, mission impact, and cost-benefit of proposed, new or revised cyber security laws, regulations, policy, requirements, etc.

g. Program Secretarial Officers (PSO).

(1) Retain overall accountability for CSP implementation within their organization.

(2) Uses DOE line management, independent oversight, and contractor assurance systems to (1) make informed decisions about corrective actions (2) assess the acceptability of risks, and (3)

improve the effectiveness and efficiency of programs and site operations. This authority may be further delegated.

(3) Ensure the applicable SDM RMA is implemented in a manner that cost-effectively reduces risks to an acceptable level.

(4) Monitor the effectiveness of RMA implementation.

(5) Serve as the AO for information systems under their purview. This authority may be further delegated. The delegating official remains responsible and accountable.

(6) Notify contracting officers of which contracts must incorporate the CRD.

h. Federal Site Manager. Oversee contractor performance.

(1) Oversee the effective management of the site cyber security program, approving, reviewing, and/or accepting CAS outputs.

(2) Oversee and review the effectiveness of the site-level RMA, communicating results and decisions with SDM and Site Contractor Management.

(3) Coordinate with Senior Site Contractor Management (e.g., Laboratory Director, Plant Manager) to codify acceptable site-level, local risk in the context of mission performance.

i. Information Management Governance Council Advisory Group (IMGCAG).

(1) Provide input and recommendations for new or revised cyber security policy.

(2) Provide recommendations to the IMGC on the applicability, mission impact, and cost-benefit of proposed, new or revised cyber security laws, regulations, policy, requirements, data calls, etc.

j. Director of the Office of Intelligence and Counterintelligence.

(1) Serve as an Advisory member of the IMGC.

(2) Serve as the AO for DOE information systems under the purview of Intelligence Community. This authority may be further delegated. The delegating official remains responsible and accountable.

(3) Ensure that intelligence systems operated by Headquarters and Field elements of the Office of Intelligence and Counterintelligence are

protected in accordance with applicable Director of National Intelligence and DOE policy and directives.

k. Chief Health, Safety and Security Officer (HSS).

(1) Serve as an Advisory member of the IMGC.

(2) Provide independent oversight of the RMA in accordance with the mission, functions, and assigned responsibilities of the Office of HSS and associated DOE directives.

l. Heads of Departmental Elements (other than those under the purview of Under Secretaries, NNSA Administrator, and the DOE CIO).

(1) Retain overall accountability for RMA implementation within their organization.

(2) Prepare and maintain an organizational RMA as described in paragraph 4 or implement the Department RMA developed and maintained by the DOE CIO.

(3) Ensure the RMA is implemented in a manner that cost-effectively reduces risk to an acceptable level.

(4) Monitor the effectiveness of RMA implementation.

(5) Serve as the AO for information systems under their purview. This authority may be further delegated. The delegating official remains responsible and accountable.

(6) Notify contracting officers of which contracts must incorporate the CRD.

m. Contracting Officers. Once notified of contractor applicability, incorporate the CRD into affected contracts.

6. REFERENCES.

a. FEDERAL LAWS AND REGULATIONS.

(1) P.L. 106-65, "National Defense Authorization Act [Section 3212(d)], enacted October 1999.

(2) P.L. 107 347, Title III, Federal Information Security Management Act of 2002 (FISMA), enacted December 2002.

b. OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULARS. Located at http://www.whitehouse.gov/omb/circulars_default/.

c. OMB MEMORANDA PERTAINING TO INFORMATION TECHNOLOGY SECURITY AND MANAGEMENT. Located at http://www.whitehouse.gov/omb/memoranda_default/.

d. DOE ORDERS, MANUALS, NOTICES, AND GUIDELINES. Located at https://www.directives.doe.gov/directives.

(1) DOE M 470.4-4A, *Information Security Manual*, dated 10-12-10.

(2) DOE O 475.2A, *Identifying Classified Information*, dated 02-01-11.

(3) DOE O 251.1C, *Departmental Directives Program*, dated 1-15-09.

(4) DOE O 206.1, *Department of Energy Privacy Program*, dated 1-16-09.

e. OTHER.

(1) 32 CFR 2001.23, Classification Marking in the Electronic Environment, dated 6-28-10.

(2) 32 CFR2001.24, Additional Information, dated 6-28-10.

(3) Atomic Energy Act of 1954 as amended.

(4) E.O. 12344, "Naval Nuclear Propulsion Program," dated 2-1-82.

(5) E.O. 13526, "Classified National Security Information," dated 12-29-09.

(6) National Security Agency/Central Security Service Storage Device Declassification Manual (SDDM), dated 12- 2007.

(7) Issuances of the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC). Index of National Security Systems Issuances can be found at www.cnss.gov/Assets/pdf/CNSS-INDEX.pdf.

(a) Committee on National Security Systems, CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*.

(b) CNSS Policy (CNSSP) 22, *Information Assurance Risk Management Policy for National Security Systems*.

(c) CNSSP 26, *National Policy on Reducing the Risk of Removable Media*.

(8) National Institute of Standards and Technology (NIST). Directory of NIST publication can be found at http://csrc.nist.gov/index.html.

(a) NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

(b) NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

(c) NIST Special Publications (NIST SP) 800 series (not all-inclusive):

1 NIST SP 800-36, Guide to Selecting Information Technology Security Products.

2 NIST SP 800-37, Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems.

3 NIST SP 800-53, Rev 3, Recommended Security Controls for Federal Information Systems and Organizations.

4 NIST SP 800-88, Guidelines for Media Sanitization.

7. DEFINITIONS. See Attachment 2.

8. CONTACT. Questions concerning this Order should be directed to the Office of the Chief Information Officer at (202) 586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

DANIEL B. PONEMAN
Deputy Secretary

Considerations for Supply Chain Risk Management in Risk Management Implementation Plans

1. Policies and procedures to assess the criticality of systems to which ICT SCRM controls must apply beyond those required by NIST SP 800-53 or CNSS 1253.

2. Policies and procedures to ~~assess~~prioritize the essential ~~the criticality of~~ components ~~within~~of critical systems for SCRM evaluation.

3. Policies and procedures to identify and understand the risk environment, including a description of the overall (identified) risk to which the supply chain is exposed.

4. Policy and processes for the documentation, control and tracking, and approval of the ~~provenance~~integrity of information technology systems and assets.

5. Policies and procedures that reflect a risk-based defense-in-depth SCRM strategy and may ~~-~~include the following:

   a. Threat and vulnerability assessment
   b. Risk Assessment and tolerance
   c. Acquisition planning, sourcing, and safeguards
   d. Evaluation of system component/service suppliers
   e. Analysis of supplier assurance practices and due diligence
   f. Product evaluation
   g. Control of the quality, configuration, and security of software, hardware, and systems throughout their lifecycles
   h. Asset management (i.e., receiving, storage, replenishment, issuing, tracking, inventory, and disposition~~al~~ of Government-owned property)
   i. Accountability, control, visibility, protection, and identification of controlled inventory items (CII)
   ~~Mitigation methodologies, including Operations Security (OPSEC) as appropriate~~
   j. Weakness/deficiency detection, reduction, and mitigation strategies
   k. Incident management
   l. Training and awareness
   m. Monitoring and reporting

6. Inclusion of ICT SCRM controls in system documentation, including design and implementation plans; threat, vulnerability, and risk assessments; System Security Plans (SSPs); and Security Testing and Evaluation (ST&E) procedures, as applicable.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD)
DOE O 205.1B, *Department of Energy Cyber Security Program*

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachments 2 and 3 to DOE O 205.1B referenced in and made a part of this CRD and which provide information to assist in the implementation of program requirements applicable to contracts in which this CRD is inserted.

1. The contractor is responsible for assessing and managing risk within its environment, in the context of acceptable mission risk set collaboratively with the Federal Site Manager.

2. The contractor must formally establish a Site Risk Management Approach (RMA) that is consistent with the requirements of the applicable Senior DOE Management (SDM) RMA implementation.

3. The contractor must establish and maintain an effective *Assurance System* that provides appropriate transparency to Federal oversight regarding cyber security risk management and overall performance.

4. The contractor must establish and implement a configuration management approach. Where mission appropriate, the approach must consider federally established configurations, such as the Federal Desktop Core Configuration (FDCC) as an alternative.

5. Where mission appropriate, or where required in the SDM RMA Implementation Plan, the contractor must consider and incorporate Federal initiatives such as HSPD-12 (or compatible) logical access capabilities and the use of Internet Protocol (IP) v6 and Domain Name System Security Extensions (DNSSEC) as part of their system development life cycle plans.

6. The contractor must establish a process to ensure that users acknowledge and consent to site privacy and monitoring policies.

7. The contractor must establish and maintain an Incident Management Handling and Reporting Capability that is consistent with the contractor requirements contained within the applicable SDM RMA Implementation plan. This capability must include:

    a. Reporting cyber security and privacy incidents to the Joint Cybersecurity Coordination Center (JC3).

    b. NNSA contractors must report cyber security and privacy incidents to the NNSA Information Assurance Response Center (NIARC).

c. If loss or unauthorized exposure of information associated with National Security Systems (NSS) is suspected, the incident must be immediately reported to the AO and JC3.

8. Contractor's NSS must adhere to the requirements established by the Committee on National Security Systems (CNSS). Requests for equivalencies and for exemptions from CNSS requirements must follow those processes, as amplified by SDM RMA implementation plan direction.

9. Contractors with NSS must implement DOE classified data protection levels as defined in their respective SDM RMA implementation plans.

10. Contractors with NSS must apply the classification markings in the electronic environment as described in the applicable SDM RMA implementation plans.

11. Contractors with NSS must implement requirements for accessing and protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Transclassified Foreign Nuclear Information (TFNI) as defined in the SDM RMA implementation plans.

12. The contractor must ensure all information systems operate within the processes defined and approved by the Federal Authorized Official, and that all systems maintain an acceptable level of risk pursuant to (1) the agreed upon risk profile defined by Site and Federal management, and (2) approved oversight and assurance systems.

DEFINITIONS

APPLICABILITY. This Attachment provides information and/or requirements associated with DOE O 205.1B as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 205.1B) is inserted.

Refer to *NIST Interagency Report (IR) 7298 Revision 1, Glossary of Key Information Security Terms* for additional definition related to cyber security, but not unique to this Order. The NIST IR 7298 Rev 1 includes most of the current terms & definitions used in NIST information security publications and those in the *CNSS Instruction No. 4009, National Information Assurance (IA) Glossary*.

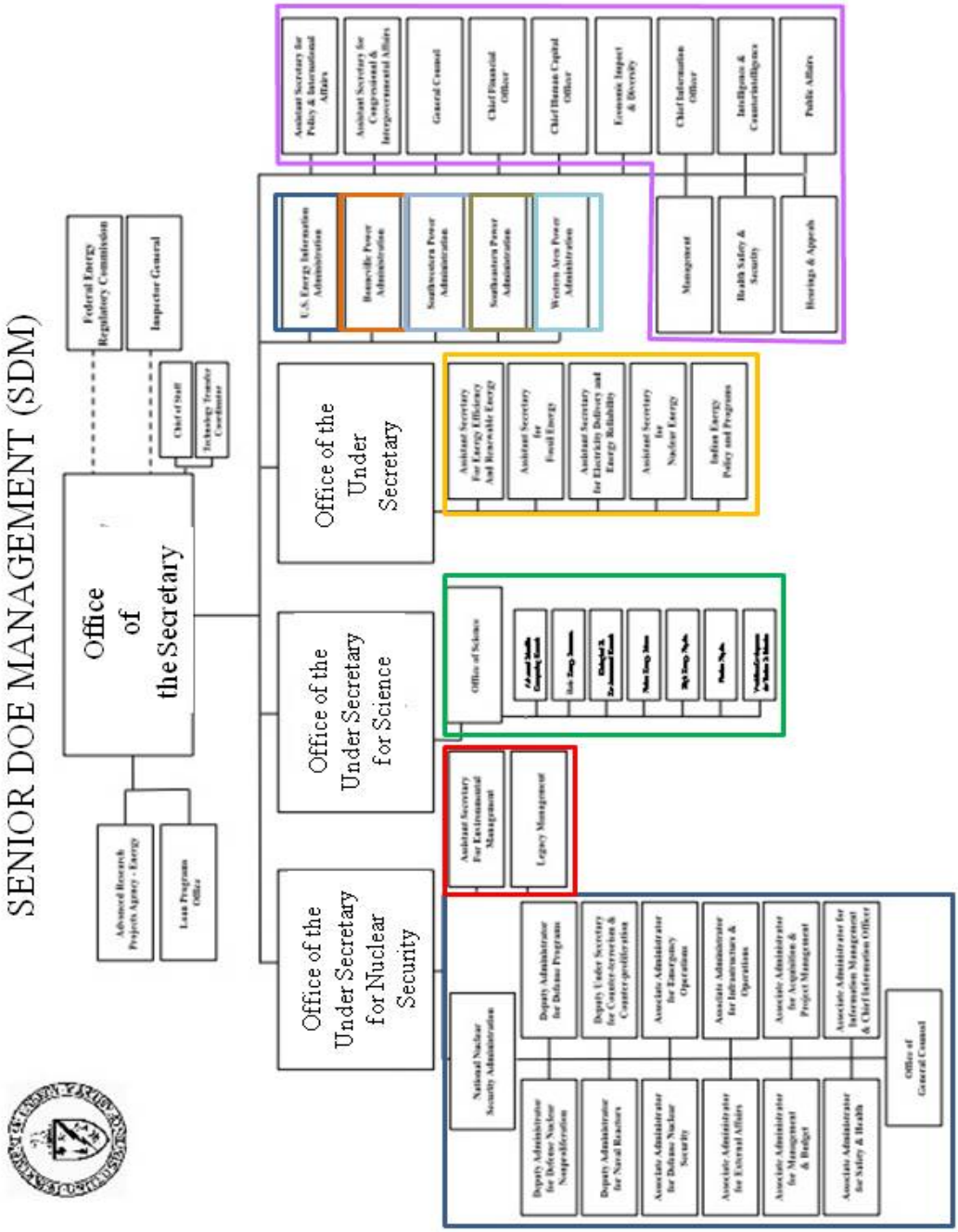
1. Advisory Member. A subject matter expert representative from the Federal Government, a DOE National Laboratory or Production Facility that officially participates on the Information Management Governance Council (IMGC), but does not have IMGC decision authority or voting privileges.

2. Assurance System. Encompass all aspects of the processes and activities designed to identify deficiencies and opportunities for improvement, report deficiencies to the responsible managers, complete corrective actions, and share in lessons learned effectively across all aspects of operation. Often referred to as Contractor Assurance System (CAS) for an M&O organization.

3. Cyber Security. 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).

4. DOE Oversight. Encompasses activities performed by DOE organizations to determine whether Federal and contractor programs and management systems, including assurance and oversight systems, are performing effectively and/or complying with DOE requirements. Oversight programs include operational awareness activities, onsite reviews, assessments, self-assessments, performance evaluations, and other activities that involve evaluation of contractor organizations and Federal organizations that manage or operate DOE sites, facilities, or operations.

5. DOE Federal System. Includes systems operated by the DOE or by contractors on behalf of the DOE where the system is used to accomplish a Federal function. Does not include systems operated by M&O contractors unless such systems meet the above definition.


SENIOR DOE MANAGEMENT (SDM)
Office of the Secretary
Federal Energy Regulatory Commission
Inspector General
Chief of Staff
Technology Transfer Coordinator
Advanced Research Projects Agency - Energy
Loan Programs Office
Office of the Under Secretary
Office of the Under Secretary for Science
Office of the Under Secretary for Nuclear Security
Assistant Secretary for Policy & International Affairs
Assistant Secretary for Congressional & Intergovernmental Affairs
General Counsel
Chief Financial Officer
Chief Human Capital Officer
Economic Impact & Diversity
Chief Information Officer
Intelligence & Counterintelligence
Public Affairs
Management
Health Safety & Security
Hearings & Appeals
U.S. Energy Information Administration
Bonneville Power Administration
Southwestern Power Administration
Southeastern Power Administration
Western Area Power Administration
Assistant Secretary for Energy Efficiency And Renewable Energy
Assistant Secretary for Fossil Energy
Assistant Secretary for Electricity Delivery and Energy Reliability
Assistant Secretary for Nuclear Energy
Indian Energy Policy and Programs
Office of Science
Assistant Secretary For Environmental Management
Legacy Management
National Nuclear Security Administration
Deputy Administrator for Defense Programs
Deputy Under Secretary for Counter-terrorism & Counter-proliferation
Associate Administrator for Emergency Operations
Associate Administrator for Infrastructure & Operations
Associate Administrator for Acquisition & Project Management
Associate Administrator for Information Management & Chief Information Officer
Office of General Counsel
Deputy Administrator for Defense Nuclear Nonproliferation
Deputy Administrator for Naval Reactors
Associate Administrator for Defense Nuclear Security
Associate Administrator for External Affairs
Associate Administrator for Management & Budget
Associate Administrator for Safety & Health