DEPARTMENT OF ENERGY

Office of the Under Secretary of Energy

ENERGY PROGRAMS IMPLEMENTATION PLAN FOR THE DEPARTMENT'S RISK MANAGEMENT APPROACH

August 2012
Version 1.0

Table of Contents

Table of Exhibits

Document Change History

Version #	Release Date	Summary of Changes	Changes Made By
0.1	9/17/2010	Initial Draft	
0.2	8/2/2011	Incorporated information DOE O 205.1B and DOE O 226.1B. Changed name from Energy PCSP to Energy Program Implementation Plan for the Department's Risk Management Approach (Energy Programs RMA IP)	S. Moore, R. Jansto A. Rahman
0.3	9/14/2011	Incorporated comments from DOE programs; GE, ED, and TE.	S. Moore I Best
0.4	11/15/2011	Incorporated comments from CAS working group and GO.	S. Moore V. Cuello
1.0	07/19/2012	Review and update of headers, titles, charts, and tables for print formatting.	J. Fry S. Moore

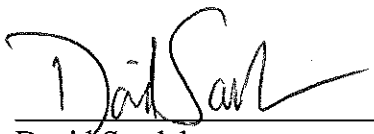
Executive Summary

The Office of the Under Secretary of Energy implementation plan for the Department's Risk Management Approach (Energy Programs RMA IP) is consistent with the Department's RMA as defined in DOE O 205.1B and defines the cyber security risk management processes, roles, and responsibilities for Energy Program Offices. The Energy Programs RMA IP provides the cyber security management requirements for Energy Program Offices and their associated field sites and laboratories, including the Office of Energy Efficiency and Renewable Energy (EE), Office of Fossil Energy (FE), Office of Nuclear Energy (NE), and Office of Electricity Delivery and Energy Reliability (OE).

The Energy Programs RMA IP utilizes national standards in defining the risk management processes and minimum baseline requirements necessary for ensuring protection of unclassified and classified information systems commensurate with mission needs. The risk management process described in the Energy Programs RMA IP is used to direct cyber security performance within the Energy Program Offices. The Energy Programs RMA IP will be periodically updated and revised as needed to reflect changes to national and departmental policy and guidance.

For Federal entities the roles and responsibilities, risk management process, and continuous monitoring process defined in the Energy Programs RMA IP are effective immediately. Program Managers and sites will ensure that contracting officers are instructed to place the Energy Programs RMA IP into affected site/facility management contracts and service contracts as appropriate. Each organization must begin implementation of the Energy Programs RMA IP within three months of issuance.

The varied missions of Energy Program Offices play a critical role in accomplishing the Department's mission to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission. I earnestly believe that effective, risk-based cyber security management plays an important role in accomplishing our mission. The Office of the Under Secretary of Energy Cyber Security Program is available to provide guidance in addressing the requirements defined in the Energy Programs RMA IP and ongoing cyber security management.



David Sandalow
Acting Under Secretary of Energy

10/2/2012
Date

1 Introduction

Pursuant to DOE Order 205.1B, *Department of Energy Cyber Security Program*[1] the Department of Energy's (DOE's) overarching mission to advance the national, economic, and energy security of the United States and promote scientific and technological innovation is enabled, advanced, and reliant on information and information systems[2], which must be adequately protected to ensure mission success. The Office of the Under Secretary of Energy is responsible and accountable for managing a cyber security program that ensures adequate protection of information and information systems within Energy Program Offices to enable the DOE mission.

The Office of the Under Secretary of Energy implementation plan for the Department's Risk Management Approach (Energy Programs RMA IP)[3], provides Energy Program Offices with implementation direction for the Department's RMA utilizing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and NIST SP 800-39, *Managing Information Security Risk.* The Energy Programs RMA IP employs a mission-focused enterprise-wide approach to securing information and information systems. The risk management processes cover the entire risk management lifecycle, providing a flexible process for cyber security risk management commensurate with mission needs. 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 Energy Program Offices.

Energy Program Offices are to use a graded, risk-based approach to security based on an analysis of threats and vulnerabilities (risks), cost and mission effectiveness, data sensitivity and organizational impact of loss or compromise. This graded approach is implemented at the system level by utilizing appropriate baselines for security controls as defined by Federal Information Processing Standard (FIPS) 199 and 200. Furthermore, this approach is also consistent with guidelines from NIST SP 800-53 Revision 3, Committee on National Security Systems (CNSS) Instruction 1253, as well as other appropriate national standards.

1.1 Purpose

The purpose of the Energy Programs RMA IP is to provide a framework for cyber security management across Energy Program Offices that is consistent, mission-focused, and based on solid risk management principles. The direction defined in this document is driven by the need to

[1] DOE O 205.1B, *Department of Energy Cyber Security Program* cancels the following: DOE O 205.1A, *Department of Energy Cyber Security Program Management*, DOE M 205.1-4, *National Security System Manual;* DOE M 205.1-5, *Cyber Security Process Requirements Manual;* DOE M 205.1-6, *Media Sanitization Manual;* DOE M 205.1-7, *Security Controls for Unclassified Information System Manual*; and DOE M 205.1-8, *Cyber Security Incident Management Manual.*

[2] As defined by OMB Circular A-130, the term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

[3] In accordance with DOE O 205.1B, the Energy Programs RMA IP cancels the Energy Program Cyber Security Plan.

enhance mission delivery, strengthen partnership among stakeholders, and satisfy Federal and Departmental requirements for cyber security management of Energy information systems. The Energy implementation of the Department's RMA meets the Departments obligations under the Federal Information Security Management Act (FISMA). This structured yet flexible approach focuses on enabling accomplishment of the varied missions of the Energy Program Offices, while providing a simple, agile, and transparent process that is consistent with NIST guidance, provides operational awareness, and utilizes site expertise.

This approach also utilizes a contractor and/or performance assurance model for functional oversight. The Energy Programs RMA IP lays out general processes and expected steps for risk management activities for Energy Program Offices. It is expected that for M&O contracts, each Contractor Assurance System (CAS) will describe, at a minimum, the areas in Section 7.0 of this document. Thus, it is understood that processes for M&O organizations with an approved CAS may vary from the processes described here, and should be performed in accordance with the relevant CAS.

1.2 Scope

The Office of the Under Secretary of Energy addresses cyber security requirements and processes outlined by Federal law and directives, DOE policy and directives, and NIST standards and guidance. All Energy Program Offices must implement the Energy Programs RMA IP and the associated requirements for cyber security management for all FISMA reportable unclassified and national security systems. Reimbursable work for outside organizations (non-DOE) may choose to, but are not required to follow Energy Programs RMA IP requirements, as the customer generally specifies the requirements for those systems. This policy applies equally to DOE organizations utilizing management and operations (M&O) contracts[4], except that it is understood that processes may vary for M&O contracts that implement a CAS as described in section 7 of this document and consistent with the oversight policy described in section 2.2.2.

Existing systems that are authorized to operate may continue operating until security authorization is required, either due to the systems' current authorizations expiring, to meet annual authorization requirements described in section 4.7 or due to a security significant change. After implementation of the Energy Programs RMA IP, all new authorizations must be completed in accordance with the Department's risk management approach as detailed within this document.

1.3 Background

The Under Secretary of Energy is committed to ensuring the long-term success of an effective cyber security program. DOE O 205.1B assigns the Under Secretary responsibility for the development of an organizational risk management approach to direct implementation of the Department's RMA for the Energy Program Offices. The Energy Programs RMA IP provides implementation direction for the Department's RMA. Each Program Office may develop, document, and implement policies and procedures in accordance with the processes and

[4] The term "M&O contract" means an agreement under which DOE contracts for the operation, maintenance, or support of Government-owned or Government-controlled research, development, special production or testing establishment wholly or principally devoted to one more major DOE programs.

requirements defined in this document and commensurate with the level of security required for the environment and unique needs of the Energy Program Offices.

1.3.1 Organizational Structure

Program offices under the purview of the Under Secretary of Energy include EE, FE, NE, and OE, as illustrated below. Each Energy Program Office, including its field sites and laboratories, is required to implement the Department's RMA as documented in the Energy Programs RMA IP.

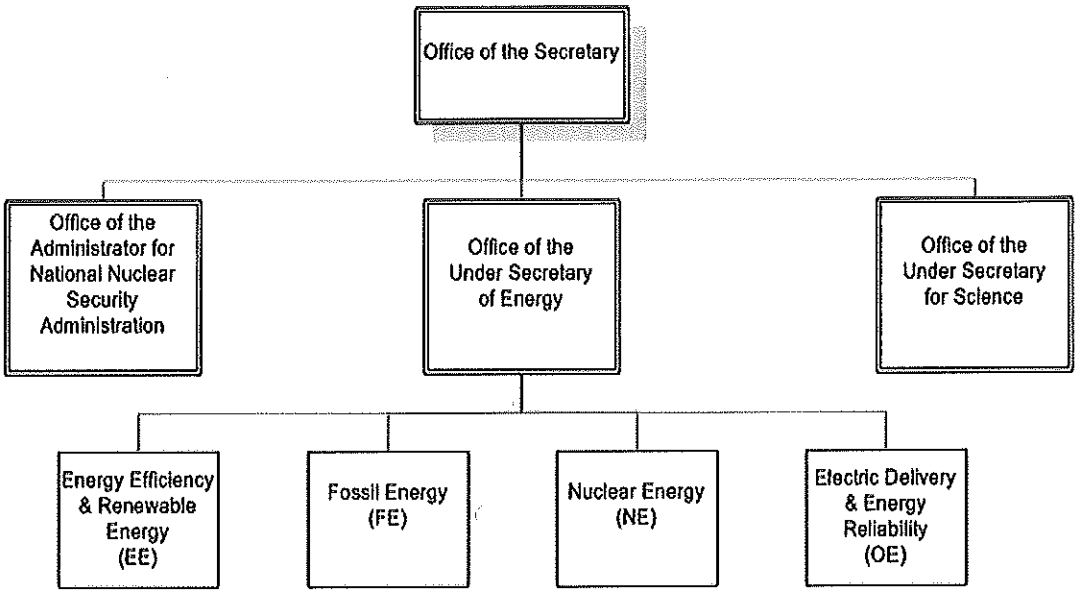


Exhibit 1: Under Secretary of Energy Organizational Chart

1.3.2 Point of Contact

Questions concerning the Energy Programs RMA IP should be addressed to the Office of the Under Secretary of Energy Cyber Security Program Manager (CSPM):

Name: Samara N. Moore
Address:
1000 Independence Avenue, SW
Office of the Under Secretary of Energy (S-3)
Washington, DC 20585
Telephone: 202-586-1283
Email: Samara.Moore@hq.doe.gov

1.4 Energy Programs RMA IP Change Management

All changes to the Energy Programs RMA IP will be vetted and managed by the Under Secretary of Energy's CSPM. The Energy CSPM will oversee the Energy Programs RMA IP through a Change Management process, reviewing the Energy Programs RMA IP at least annually for validity.

The Document Change History table is used to record information for controlling and tracking modifications made to this document. As the versions are updated, the Office of the Under Secretary of Energy notifies the Energy Program Offices of the updates. New versions are reissued to the cyber security community for review and comment, as appropriate. The Under Secretary of Energy approves all final changes to this document.

2 Cyber Security Governance

Cyber security governance focuses on the oversight of high-level outcomes and the outputs of the Performance Assurance System. The goals of cyber security governance are to:

- Provide strategic direction;
- Ensure that organizational mission and business objectives are achieved;
- Ensure that risks are managed appropriately; and
- Verify that organizational resources are used responsibly.

2.1 Risk-based Approach to Cyber Security Governance

Cyber security management decisions should be based on an organization-wide, mission focused risk-based process. The establishment and utilization of a Risk Executive (Function) with an enterprise-wide perspective of risk management and an understanding of the mission needs is an essential component of the Department's cyber security governance model.

Outcomes of the application of an organization-wide, risk-based approach to governance include:

- Strategic alignment of risk management decisions with critical missions and business functions consistent with organizational goals and objectives;
- Execution of risk management processes to frame, assess, respond to, and monitor risk to organizational operations and assets, individuals, and other organizations;
- Effective and efficient allocation of risk management resources;
- Performance-based outcomes by measuring, monitoring, and reporting risk management metrics to ensure that organizational objectives are achieved;
- Delivered value by optimizing risk management investments in support of organizational objectives; and
- Performance assurance for M&O contracts through the Contractor Assurance System (CAS).

2.2 Energy Program Oversight and Assurance

To guide the implementation of the appropriate oversight and assurance within Department elements, DOE O 226.1B, *Implementation of Department of Energy Oversight Policy* details an assurance model in which (1) Headquarters line management provides direction and oversight to line management in the field and evaluates implementation of Headquarters expectations and effectiveness of field element line management; (2) Field line management conducts direct oversight of contractor activities, work controls and procedures to meet mission objectives and contractual obligations; and (3) Independent oversight is performed by the DOE Office of Independent Oversight and other organizations that are independent from DOE line management.

Consistent with DOE O 226.1B, cyber security oversight and assurance for Energy Program Offices shall be accomplished through line management directed assessments, confirmation of contractor assurance systems, and internal and external reviews. This approach relies on a close partnership between DOE headquarters, the local site office, and the contractor (for Government-owned/contractor-operated sites, or M&O contractors) or Federal organization (for Government-owned/Government-operated sites). In this partnership, the contractor provides assurance to DOE that is transparent and allows DOE to leverage the contractor's (or Federal organization's) processes and outcomes, and confirm their effectiveness. Organizations shall establish an oversight program consistent with DOE O 226.1B.

Additionally, DOE Policy requires all Departmental organizations to implement assurance systems that ensure compliance with applicable requirements; pursue excellence through continuous improvement; provide for timely identification and correction of deficient conditions; and verify the effectiveness of completed corrective actions.[5] Pursuant to DOE O 205.1B and DOE O 226.1B, this section defines a process for developing minimum required components of applicable assurance systems, such as risk tolerance, and/or performance indicators, objectives, measures, and others.

DOE oversight encompasses activities 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.

The Performance 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 effectively share lessons learned across all aspects of operation.

Requirements for the Energy Program's Performance Assurance System include:

- Assessments, including self-assessments, management assessments, and internal or directed independent assessments;
- Incident/Event reporting processes;
- Worker feedback mechanisms;
- Issues management with corrective action tracking, closure, and validation;
- Lessons learned; and
- Performance measures to demonstrate performance improvement or deterioration relative to identified goals.

The Energy Program Office cyber security oversight model is conducted through a Performance Assurance System that monitors the risk evaluation and protection processes at each level in the organization. It also provides a mission-based methodology for graded oversight that is based on

[5] DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*

risk and the contractor's opened system risks identified in an updated Plan of Action and Milestones (POA&Ms).

2.2.1 Under Secretary of Energy Oversight of Programs

DOE O 226.1B requires Senior DOE Management (SDM) to maintain operational awareness and oversee the development, implementation, and maintenance of applicable assurance systems. By developing and promulgating the policy/framework described in the Energy Programs RMA IP, the Office of the Under Secretary of Energy provides Energy Program Offices with the direction necessary to implement appropriate, risk-based, cyber security assurance mechanisms. The direction provided in the Energy Programs RMA IP provides a high level oversight strategy by which Energy Program Offices can ensure effective implementation of the Energy Programs RMA IP within the Energy Program Offices, as well as a mechanism for feedback, issues management, and tracking of required corrective actions. Section 7 of this document addresses the Contractor Assurance System, and implements Attachment 1 (CRD) of DOE O 226.1B. The CAS is a critical component of Energy's program oversight that allows M&O contractors to manage systems based on risk, and with defined processes and touch points to support transparency and Government oversight.

2.2.2 Program Secretarial Office Oversight

The Energy Program Offices (PSOs) ensure application of the Energy Programs RMA IP and coordinate with site offices to ensure applicable line management and contractor entities develop and provide assurance systems with performance measures requisite with Office of the Under Secretary of Energy requirements, and conversely, that feedback provided by assessors and Senior DOE management for corrective actions, lessons learned, and opportunities for improvement are addressed and implemented.

Energy Program Offices will also work with contracting officers to ensure that contractor award fees for contracts have the appropriate language for ensuring that the Energy Programs RMA IP is included in the appropriate contracts and considered in the award determination. Therefore, program managers must make certain the contract award fees meet the following criteria:

- Contract award fee determinations must include an evaluation of cyber security effectiveness with a weight or importance at least commensurate with that of physical security or safety in each contract; and
- Appropriate cyber security-related incentives and disincentives are identified and implemented for those sites and contractors without award fees.

Within the Energy Program Offices, the appropriate authorizing official (AO) must, in coordination with applicable contracting officials, define processes to evaluate contractor programs, management, and assurance systems, for effectiveness of performance, and consistent with DOE O 226.1B.

2.2.2.1 Performance Metrics

The Office of the Under Secretary will establish high level performance measures to maintain operational awareness and cognizance of the residual risk.

Within specific programs and sites, promulgation of assurance requirements will be measured via the development and implementation of contractor assurance systems (CAS) into applicable contracts. These CAS's must be aligned with the Energy Programs RMA IP, and must fulfill the requirements described in DOE O 226.1B. Additional guidance for the development of meaningful information security performance metrics can be found in NIST SP 800-55, *Performance Measurement Guidance for Information Security.*

2.2.2.2 Contractor Requirements Document

The contractor requirements document (CRD) of DOE O 205.1B sets forth the requirements of DOE O 205.1B for management and operating (M&O) contracts. However, support service contracts must also manage DOE information security in accordance with the Energy Programs RMA IP.

Timeframes for including the 205.1B CRD into M&O contracts is as follows:

- Existing contracts – The process to modify existing contracts with the 205.1B CRD should begin within 90 days of the issuance of the Energy Programs RMA IP.
- New contracts – The 205.1B CRD should be included immediately in all new contracts.

Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the requirements of 205.1B. 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.

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.

2.3 Assessments

The Energy Program Office oversight strategy includes self and independent assessments, whether they be management directed, self-initiated, or from a third party such as the Inspector General or the Office of Health, Safety, and Security. These assessments include continuous monitoring of the information system. Cyber security assessments may be performed at the request of the site office manager, Program Office, or the Office of the Under Secretary, and can be used as an independent evaluation of the cyber security program. Authorizing Officials must define the appropriate level of independence for cyber security assessments, but in general, NIST defines independent assessments as follows:

> "An independent assessor or assessment team is an individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. The authorizing official determines the required level of assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets, and to individuals. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results."[6]

Weaknesses discovered during assessments (self or independent) should be recorded as site, system, or program weaknesses and tracked in the appropriate plans of actions and milestones (POA&Ms). POA&Ms should contain detailed corrective actions, milestones and schedules, and be recorded in DARTS where appropriate. For M&O contracts, the system authorization process defined in the CAS must define the type and frequency of required assessments, acceptable levels of independence (if needed), and processes required for weakness tracking, reporting and remediation.

3 Roles and Responsibilities

This document expands upon roles and responsibilities described in 205.1B and NIST SP 800-37 Revision 1 to further define those roles specific to Energy Program Offices.

The Energy Programs RMA IP also builds on the cyber security awareness and training requirements baseline described in NIST SP 800-53 Revision 3. The DOE workforce (both DOE Federal and contractor) should also focus on developing and maintaining proper organizational threat awareness, risk management, and cyber security posture for their specific role.

3.1 Under Secretary of Energy

Brief Description: The Under Secretary of Energy provides assurance that the Department is achieving its missions effectively and efficiently with reasonable risk, and retains overall responsibility and accountability for the Energy Implementation of the Department's RMA. The Under Secretary codifies acceptable residual risk, balancing mission performance with cost and risk. In accordance with this responsibility to establish the organizational tolerance for risk, the

[6] NIST SP 800-53 rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, page F-33 (control CA-2(1))

Under Secretary also establishes guidance on how risk tolerance influences ongoing decision-making activities as well as communicates acceptable mission risk to Federal Site Management, Energy Program Contracting Officer(s) (CO), and the Senior Contractor Official Responsible for Cyber. The Under Secretary also develops and maintains the Energy Programs RMA IP in accordance with 205.1B, and flows down the requirements and responsibilities of this Order to all Energy Program Offices through the Energy Programs RMA IP. Requirements for M&O contractor assurance also flow down and are described by the CAS. He/she also notifies the Energy Program Office COs regarding which contracts must incorporate the CRD, as well as establishing and implementing an effective oversight program consistent with requirements defined in DOE O 226.1B, and detailed in the CAS for M&O contractors.

The Under Secretary also serves as a member of the Information Management Governance Council (IMGC), coordinates with the DOE CIO in the development of the Energy Programs RMA IP, and coordinates with the IMGC to resolve cross SDM issues. Additionally, the Under Secretary serves as the Authorizing Official (AO) for information systems under their purview. While this authority may be further delegated within the organization, the delegating official remains responsible and accountable.

The Under Secretary of Energy may delegate a number of responsibilities to each of the respective Program Secretarial Offices (PSOs). These include: 1) serving as the AO for the specific Energy Program office, and 2) notification of which contracts must include the CRD from 205.1B.

3.2 Under Secretary of Energy Cyber Security Program Manager

Brief Description: The agency official responsible for: (i) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements within the Office of the Under Secretary of Energy; (ii) assisting the Under Secretary of Energy and other senior organizational officials concerning their security responsibilities; and (iii) in coordination with other officials, reporting annually to the Under Secretary of Energy on the overall effectiveness of the organization's information security program, including progress of remedial actions. The Under Secretary of Energy Cyber Security Program Manager (CSPM) will maintain operational awareness of Energy program office cyber security posture via periodic reviews and oversight actions.

3.3 Program Secretarial Officer

Brief Description: The Program Secretarial Officer (PSO) retains overall accountability for implementing the Energy Programs RMA IP within their organization in a manner that cost-effectively reduces risks to an acceptable level. The PSO in-turn monitors the effectiveness of the Energy Programs RMA IP implementation, doing so by using 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, as necessary. The PSO will work with the CO to address important contracting procedures. The PSO will notify the CO regarding which contracts must incorporate the 205.1B CRD. The PSO

also serves as the AO for information systems under their purview. This authority may also be further delegated. However, the delegating official remains responsible and accountable.

The Under Secretary of Energy delegates to each of the PSOs a number of responsibilities, including: 1) serving as the AO for all information systems under their purview, and 2) notifying the Energy Program CO regarding which contracts must incorporate the CRD from 205.1B. The AO responsibility may be further delegated, as necessary. However, the delegating official remains responsible and accountable.

3.4 Federal Site Manager

Brief Description: The Federal Site Manager has overall responsibility for effectively managing the site-level cyber security program, including the review and effectiveness of the site-level Energy Programs RMA IP, and coordinating with Senior Site Contractor Management (e.g., Laboratory Director, Plant Manager) to codify acceptable site-level, local risk in the context of mission performance. Establishing the acceptable level of risk for the organization must utilize a partnership approach that includes the Federal Site Manager in consultation with the Senior Site Manager, and others as appropriate, and is achieved via the CAS. Also the responsibility of the Federal Site Manager is to communicate local results and decisions with the Office of the Under Secretary of Energy and Site Contractor Management as defined by the mutually agreed upon CAS; reviewing, and/or accepting outputs from the CAS; and overseeing the overall performance of site contractors.

3.5 Senior Information Security Officer

Former Energy Equivalent: Program Office Cyber Security Program Manager
Brief Description: An agency official responsible for: (i) carrying out the chief information officer security responsibilities under FISMA for an Energy Program Office; and (ii) serving as the primary information security liaison for the Under Secretary of Energy CSPM to the organization's Authorizing Officials, information system owners, information system security managers and information system security officers. The Energy Program Office Senior Information Security Officer (SISO) ensures that the Energy Programs RMA IP is implemented within his/her Energy Program Office.

3.6 Authorizing Official

Former Energy Equivalent: Designated Approving Authority
Brief Description: A senior agency official or executive appointed by the Head of Agency with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to the organization's operations and assets, individuals, other organizations, and the Nation. AO typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. At a minimum, the AO must hold a DOE L Clearance (must be cleared to the level required to view threat information).

The AO must, in coordination with the applicable contracting officials, Risk Executive and Cyber Program Manager define processes to evaluate contractor programs, management, and assurance systems, for effectiveness of performance, and consistent with DOE O 226.1B.

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 by a "system by system" authorization. For NSS, the Federal AO function is accomplished through DOE Oversight and must be consistent with CNSS policy.

3.7 Authorizing Official Designated Representative

Former Energy Equivalent: Designated Approving Authority Representative
Brief Description: An agency official that acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process. The only activity that cannot be delegated to the Authorizing Official Designated Representative (AODR) by the AO is the authorization decision and signing of the associated authorization decision document.

3.8 Senior Contractor Official Accountable for Cyber

Brief Description: A senior contract official or executive that makes authorization recommendations to the AO. This official is responsible for operating M&O information systems at an acceptable level of risk to the organization's operations and assets, individuals, other organizations, and the Nation. The Senior Contractor Official Accountable for Cyber is responsible for managing the risk posture of the system and continuous monitoring activities including understanding weaknesses, their potential impact, and corrective action plans. In addition, this official manages the implementation of the Contractor Assurance System for any systems under his or her purview. At a minimum, the Senior Contractor Official Accountable for Cyber must hold a DOE L Clearance (must be cleared to the level required to view threat information).

3.9 Risk Executive (Function)

Brief Description: An individual or group that helps to ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions for those systems, are viewed from a enterprise-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) ensuring management of risk from individual information systems is consistent across the enterprise, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. Depending on the organization, this function may be performed by individuals or groups of individuals including the AO, System Owners, Lab Directors, Mission Executives, and others.

Risk executive functions are implemented at multiple layers such as departmental (e.g. OCIO), programs, field sites and laboratories. This new role directly supports the risk management paradigm of ensuring mission owners - Senior DOE Management, lab directors, business owners, etc. – are fully aware of, and participate in high level risk management decisions. Activities of the Risk Executive (Function) may include:

- Establishing risk management roles and responsibilities;
- Developing and implementing an organization-wide risk management strategy that guides and informs organizational risk decisions;
- Managing threat and vulnerability information with regard to organizational systems and the environments in which the systems operate;
- Establishing organization-wide forums to consider all types and sources of risk (including aggregated risk);
- Determining organizational risk based on the aggregated risk from the operation and use of information technology and industrial control systems and the respective environments of operation;
- Providing oversight for the risk management activities carried out by organizations to ensure consistent and effective risk-based decisions;
- Developing a greater understanding of risk with regard to the strategic view of organizations and their integrated operations;
- Establishing effective vehicles to serve as a focal point for communicating and sharing risk-related information among key stakeholders internally and externally to organizations;
- Specifying the degree of autonomy for subordinate organizations permitted by parent organizations with regard to framing, assessing, responding to, and monitoring risk[7];
- Promoting cooperation and collaboration among stakeholders to include security actions requiring shared responsibility;
- Ensuring that security decisions consider all factors necessary for mission and business success; and
- Ensuring shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision-making stakeholders.

3.10 Information System Owner

Former Energy Equivalent: System Owner
Brief Description: An individual responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The information system owner is responsible for addressing the operational interests of the user community (i.e.,

[7] Because subordinate organizations responsible for carrying out derivative or related missions may have already invested in their own methods of framing, assessing, responding to, and monitoring risk, parent organizations may allow a greater degree of autonomy within parts of the organization or across the entire organization in order to minimize costs. When a diversity of risk management activities is allowed, organizations may choose to employ, when feasible, some means of translation and/or synthesis of the risk-related information produced from those activities to ensure that the output of the different activities can be correlated in a meaningful manner.

users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements.

3.11 Information System Security Manager

Brief Description: A role that has oversight responsibilities for the information security program of a single or multiple information systems. The Information System Security Manager (ISSM) is considered the lead cyber security person at a field site or major contractor entity and has working knowledge of system functions, cyber security policies, and technical cyber security protection measures.

3.12 Information System Security Officer

Brief Description: An individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner and ISSM. The Information System Security Officer (ISSO) also serves as an advisor on all matters, technical and otherwise, involving the security of an information system.

3.13 Contracting Officer

Brief Description: The CO works in conjunction with the PSO to ensure and monitor contractor implementation of cyber security requirements as directed in the CRD of 205.1B. The CO works with the PSO to address the following contracting procedures:

- Review all contracts before they are awarded to ensure information security requirements have been incorporated;
- Ensure that at the expiration of a contract, all contractors must follow all DOE policies on media protection;
- Ensure that appropriate policies and procedures of external third parties are documented, agreed to, implemented, and monitored for compliance. All contractors using DOE systems must sign a Non-Disclosure Agreement and comply with DOE security policies;
- Develop and implement an information security contract clause to be enforced against all relevant DOE contracts; and
- Write specialized security requirements into the contract statements of work or professional services contracts.

The CO is notified by the Office of the Under Secretary of Energy (or PSO if delegated as such) regarding which contracts must incorporate the CRD. Once notified of this, the CO incorporates the CRD into affected contracts.

3.14 Information Owner/Steward

Brief Description: An individual with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. Information owners/stewards provide input to information system owners, ISSMs, and ISSOs regarding the security requirements and security controls for the information system(s) where the information is processed, stored, or transmitted.

3.15 Security Control Assessor

Former Energy Equivalent: Security Control Assessor
Brief Description: An individual responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls. Security Control Assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. Security Control Assessors prepare the final security assessment report containing the results and findings from the assessment.

3.16 Roles and Responsibilities Matrix

Exhibit 2 below, *Roles and Responsibilities Separation of Duties Matrix*, depicts which roles can be shared by the same person. A green ✓indicates the role can be shared by the same person. A red X indicates the roles cannot be shared by the same person based on the best practices of separation of duties. The Under Secretary, Under Secretary CSPM, SISOs, AOs, and AO Representatives must be Federal Employees.

Federal Employee Required?		UnderSec	UnSecE CSPM	SISO	AO	AODR	Risk Executive Function	System Owner	ISSM	Information Owner/ Steward	Security Control Assessor
Yes	UnderSec		X	X	✓	X	✓	✓	✓	✓	✓
Yes	UnSecE CSPM	X		X	✓	✓	✓	✓	✓	✓	✓
Yes	SISO	X	X		✓	✓	✓	✓	✓	✓	✓
Yes	AO	✓	✓	✓		X	✓	✓	✓	✓	X
Yes	AODR	X	✓	✓	X		✓	✓	✓	✓	X
No	Risk Executive Function	✓	✓	✓	✓	✓		✓	X	✓	X
No	System Owner	✓	✓	✓	✓	✓	✓		✓	✓	X
No	ISSM	✓	✓	✓	✓	✓	X	✓		✓	✓
No	Information Owner/ Steward	✓	✓	✓	✓	✓	✓	✓	✓		X
No	Security Control Assessor	✓	✓	✓	X	X	X	X	✓	X	

Exhibit 2: Roles and Responsibilities Separation of Duties Matrix

4 Implementation Requirements

The purpose of the Department's RMA is to provide a mission focused, risk-based framework for cyber security management. The RMA is driven by the business/mission requirements which are used to tailor cyber security requirements to cost-effectively reduce information security risks to an acceptable level. The Department's RMA focuses on supporting accomplishment of the varied missions of Energy Program Offices, providing a simple, agile, and transparent process, consistent with NIST guidance. It addresses all phases of the Security Authorization (SA) life cycle and introduces several changes to cyber security life cycle management.

The Office of the Under Secretary of Energy designed the Energy Programs RMA IP for the Department's RMA to address all relevant security areas outlined by Federal law and directives, DOE policy, DOE guidance, and NIST guidance including NIST SP 800-37 Revision 1. All Energy Program Offices must utilize the Energy Programs RMA IP. The Department's RMA described below and implemented by the Energy Programs RMA IP covers all information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the Energy Program Offices.

The Department's RMA (and the associated Energy Programs RMA IP) aligns with both NIST SP 800-37 Revision 1 and NIST SP 800-39. In addition to ensuring that cyber security actions are properly evaluated based on organizational risk (Step 0), the Department's RMA aligns with NIST SP 800-37 Revision 1 by providing processes for: categorizing information systems (Step 1); developing a mission-adjusted baseline of security controls (Step 2); implement (or obtain deviations from) selected security controls as necessary (Step 3); assessing these security controls (Step 4); performing information system authorizations (Step 5); and (6) implementing a continuous monitoring process (Step 6).

Additionally, as described in NIST SP 800-39, the Department's RMA implements the four components of the risk management lifecycle: risk framing; risk assessing; risk responding; and risk monitoring. Risk framing and risk assessment are completed in partnership with the DOE oversight function. Risk response ensures the defensive protections are adequate for the agreed upon risk profile. Exhibit 3 below, *Steps of the Risk Lifecycle and Energy RMA IP*, shows the four components of the risk management lifecycle with the corresponding steps of the Energy Programs RMA IP.

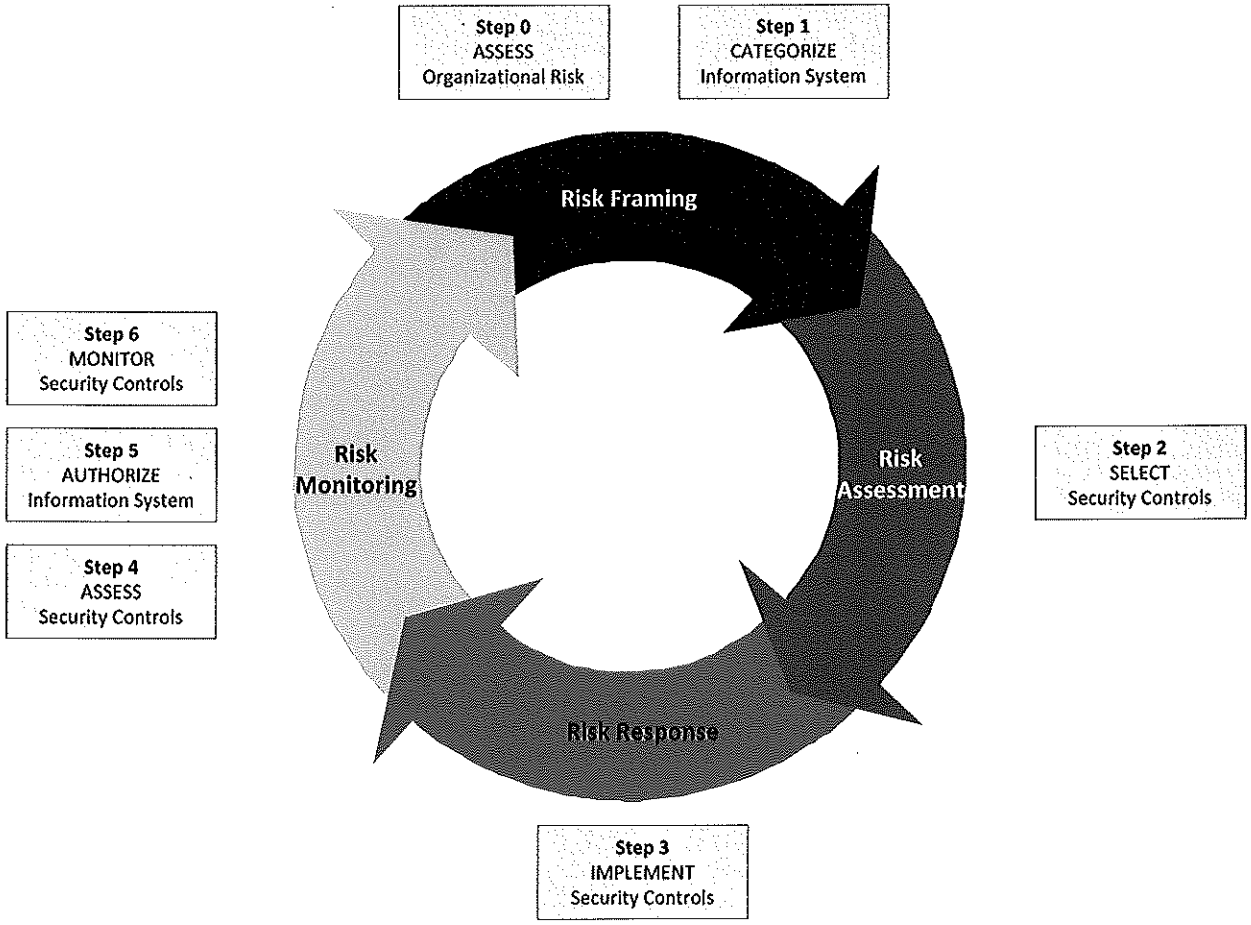


Exhibit 3: Steps of the Risk Lifecycle and Energy Programs RMA IP

4.1 Requirements

Organizations within the Office of the Under Secretary of Energy must implement cyber security management requirements as defined in DOE Directives and applicable laws and regulations. For unclassified information systems FIPS 199 and 200 must be implemented, and CNSS 1253 must be implemented for National Security Systems. All other NIST SP-800 series publications should be considered as guidance.

Additionally, 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 version 6 (IPv6), Domain Name System Security Extensions (DNSSEC) be implemented as part of system development life cycle plans.

4.2 Organizational Impact Assessment

This step aligns with Step 0 of the RMA, *Assess Organizational Impact Level.* The general concept of an Organizational Impact Assessment is outlined in NIST SP 800-37 Revision 1, but the specific steps to analyze and develop a documented output are not explicitly defined. According to NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, organizations must "determine information protection needs arising from the defined mission/business processes." In order to better align these protection needs with an organization's defined business processes, senior mission stakeholders must be involved. By first assessing impact at the organization level prior to an assessment being made at the functional IT level, one ensures that subsequent risk management decisions, including selection of controls, will better align with and support the overall mission of the organization. To ensure that risk is properly and consistently characterized and managed across the organization, it is critical that the Risk Executive (Function) is properly established and utilized within the organization.

This first step of the RMA is to develop an Organizational Impact Statement (OIS). This step consists of a four part process, described in 4.2.3, designed to gather input from mission stakeholders, analyze applicable impacts, and develop an OIS.

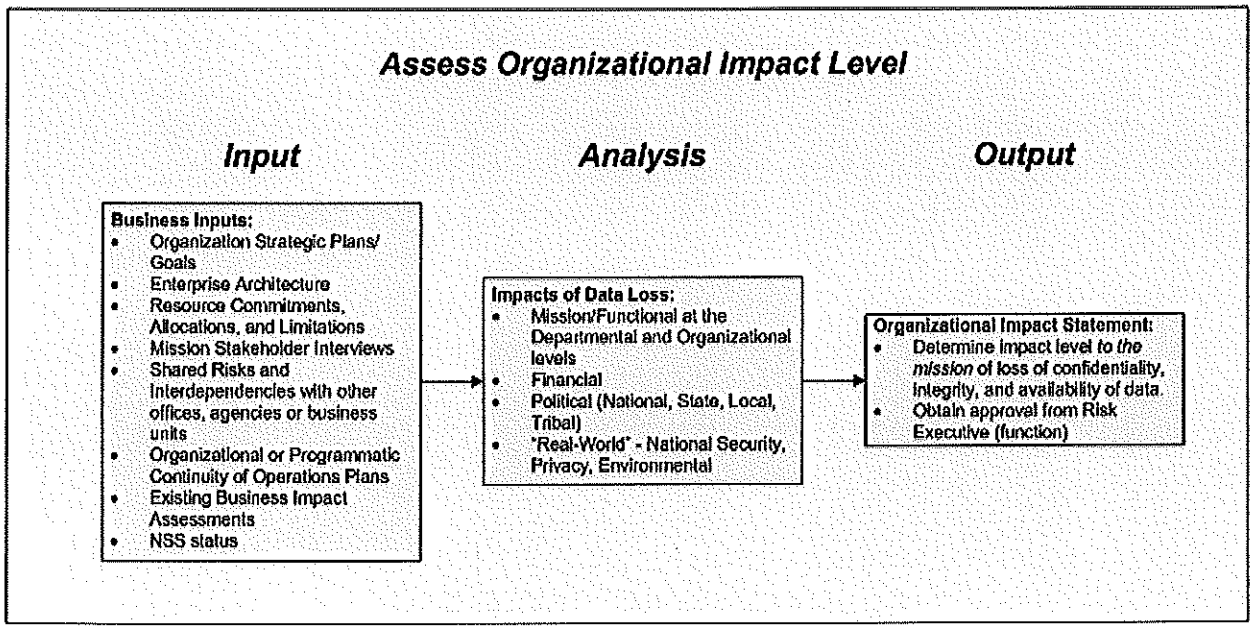


Exhibit 4: Overview of Assessing Organizational Impact Level

This OIS should represent a hybrid assessment of strategic risk from the Tier 1 and Tier 2 levels described in chapter 2 of NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.* As stated in, NIST SP 800-37 Revision 1, there may be different priorities associated with organizational missions and business processes (including derivative or related missions and business processes) that need to be factored into risk calculations - both within specific elements of the organization as well as for the overall risk

tolerance of the organization. Establishing the acceptable level of risk for the organization must utilize a partnership approach that includes the Federal Site Manager in consultation with the Senior Site Manager, and others as appropriate.

Pursuant to 205.1B, the Office of the Under Secretary of Energy "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." The Energy Programs RMA IP is how the Under Secretary establishes and communicates risk tolerance. Subsequent risk management decisions made by the Energy sites, including system categorization and selection of controls, should be guided by the Under Secretary risk guidance, as well as the subsequent OIS, which is developed by the specific Energy site. Energy organizations implementing a CAS should establish and implement site-specific risk tolerance according to the CAS.

4.2.1 Business Dependencies

This initial step defines an organization's strategic dependency on information systems by researching mission and function statements, business impact assessments, continuity of operations plans, laws, directives, policy guidance, and in-depth interviews with key stakeholders. The Risk Executive (function) should gather as much relevant background information pertaining to these dependencies as possible. The goal of this step is to develop a high level, comprehensive understanding of an organization's strategic dependency upon information systems and the program data therein. This information will be used to help mission stakeholders determine potential organizational impacts and potential risk to the organization based on the loss of the confidentiality, integrity, or availability (C-I-A) of information.

Key areas of focus should include, but are not limited to:

- Organization Strategic Plans/Goals
- Enterprise Architecture and the Systems Development Lifecycle
- Resource Commitments, Allocations, and Limitations
- Mission Stakeholder Interviews
- Shared Risks and Interdependencies with other offices, agencies or business units
- Organizational or Programmatic Continuity of Operations Plans
- Existing Business Impact Assessments
- Identification as a National Security System (NSS), additional focus areas for NSS include:
    - Safeguards and Security Site Plan
    - Memorandum of Understanding/Agreements (MOU/A)
    - Requirements Document
    - System Interconnections

4.2.2 Organizational Impact Analysis

The Risk Executive (function) along with senior business stakeholders should identify derivative impacts stemming from the loss of the C-I-A of information systems and related mission data. It is imperative that senior mission stakeholders take part in determining these functional mission impacts. This determination of high level C-I-A impact generally falls outside the realm of an IT

organization, and differs from the lower level Business Impact Assessment described in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* which correlates specific system components with the services they provide, and characterizes the consequences of downtime of those system components.

Three levels of *potential impact* on an organization's mission or business function can be assessed should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) on the information systems supporting that mission or business function.

The *potential impact* is **LIMITED** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on fulfillment of the mission or business function.

*AMPLIFICATION: A **limited** adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.*

The *potential impact* is **SERIOUS** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on fulfillment of the mission or business function.

*AMPLIFICATION: A **serious** adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals **exceeding mission expectations**.*

The *potential impact* is **SEVERE** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on fulfillment of the mission or business function.

*AMPLIFICATION: A **severe or catastrophic** adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals **exceeding mission expectations**.*

Types of impacts to be considered for the Organizational Impact Assessment should include: (i) acquisition impact (cost, schedule, performance); (ii) compliance and regulatory impact; (iii) financial impact; (iv) legal impact; (v) operational (mission/business) impact; (vi) political impact; (vii) program/project impact; (viii) reputational impact; (ix) safety impact; (x) strategic planning impact; and (xi) supply chain impact.

4.2.3 Organizational Impact Statement

As stated in NIST SP 800-53 Revision 3, information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy.

Senior mission stakeholders should formally analyze potential impacts of data loss to the organization's mission and the system's criticality to the mission. The Risk Executive (function) should weigh the system's mission criticality (gathered as Business Dependencies) versus potential impacts of data compromise (gathered during the Organizational Impact Analyses). The resulting analysis will result in a summary of Organizational Impacts based upon the potential compromise of supporting information systems.

The OIS should describe the business function supported by the system (or group of systems), and the mission impact (SEVERE, SERIOUS, LIMITED) in the event of a loss of C-I-A of that system(s). This high level summary should be approved by the organizational Risk Executive Function. An organization may elect to require additional approvals as well. This analysis, which should be documented, updated, and referenced throughout the life of the mission, will ensure that strategic, mission informed, risk-based decisions are made in the selection, maintenance, and monitoring of appropriate controls.

Specifically, the OIS should be used for determining:

- Initial system categorization as described in 4.3.1and 4.3.2;
- Mission-adjusted baseline as described in section 4.4 (to include control tailoring, scoping, common and hybrid control determinations); and
- Mission-adjusted baseline for common controls as described in 4.5.2.

4.3 Information System Categorization

4.3.1 System Categorization for Unclassified Information

This step aligns with Step 1 of the RMA, *Categorize Information Systems.* FIPS 199, the mandatory security categorization standard, is predicated on a simple and well- established concept: determining appropriate security priorities for organizational information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system must be commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation should there be a loss of confidentiality, integrity, or availability.

The security categorization process is carried out by the information system owner, information system security manager, and information owner/steward in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or risk management responsibilities). The security categorization process is conducted as an organization-wide activity, and should use the Organizational Impact Assessment to ensure that individual information systems are correctly categorized based on the system's data types within the context of the mission and business objectives of the organization.

The results of the security categorization process influence the selection of appropriate security controls for the information system, including the *Initial Baseline* and the *Mission-Adjusted Baseline*. To begin, an organization must determine the data types stored, maintained, and disseminated within the information system. Using NIST SP 800-60 as a guide, the Information System Owner and Information System Security Manager should develop a provisional categorization (i.e., impact levels for Confidentiality, Integrity, and Availability) for each data type processed by the system.

As stated in NIST SP 800-60, organizations should review and adjust the provisional security impact levels for the security objectives of each information type to arrive at a finalized state. To accomplish this, organizations should:

- Review the appropriateness of the recommended impact levels provided in NIST SP 800-60; and
- Adjust the security objective impact levels as necessary based on the organization, environment, mission, use, and data sharing impacts detailed in the Organizational Impact Assessment.

For example, if the Organizational Impact Assessment determines that the organization has placed a higher importance on availability based on mission need, the recommended *availability* impact rating of 800-60 data types should be assessed to determine if the recommended impact levels should be adjusted. This will result in a more appropriate *Initial Baseline* selection to better protect the organization's data and assets.

For the overall system categorization, the potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information processed, stored, or transmitted by those information systems. This "high watermark" of the system categorization determines the *Initial Baseline* of security controls.

4.3.2 System Categorization for NSS

Potential impact levels for integrity and availability are determined based on a risk-based assessment of data protection needs as defined in CNSS 1253. Once the impact-based security of the system has been categorized, organizations may conduct a risk adjustment to the categorization based on the results of a risk assessment or the system's environment. Data protection levels may be defined in MOU/A for system interconnections or work for others (WFO), in such cases the ability to conduct risk adjustments may be limited.

The "high watermark" concept is no longer applied for overall system categorization. Rather, the NSS system categorization reflects the potential impact values for each of the security objectives (Confidentiality, Integrity, and Availability) independently.

All security categorization decisions should be documented in the appropriate System Security Plan for unclassified information systems and NSS. Further tailoring of individual controls from the *Initial Baseline* is described in the following section.

Categorizing NSSs must use the information types and their indicated hierarchical protection levels to guide risk-based decisions. For classified systems the AO establishes, based on risk acceptance, the appropriate level of controls required to authorize use of these systems. Table D-1 of CNSSI 1253 maps the information classification levels from Executive Order (E.O.) 13526 and 10 CFR part 1045 (Confidential, Secret and Top Secret) to the CNSS 1253 potential impacts of Low, Moderate and High.

4.4 Development of the Mission-Adjusted Minimum Baseline of Security Controls

This step aligns with Step 2 of the RMA, *Select Security Controls.* The RMA gives organizations the ability to tailor controls from the *Initial Baseline* defined in NIST SP 800-53 Revision 3 for each FIPS 199 impact level. By using the Control Tailoring Process, organizations have the ability to tailor this *Initial Baseline* to produce the system's *Mission-Adjusted Baseline.*

The OIS provides an impact rating for confidentiality, integrity, and availability based upon an analysis of mission needs and objectives. The system categorization process provides security impact ratings based on the data types identified using the NIST SP 800-60 process and is aligned with FIPS 199, and the OIS. Together the output of these steps provides a framework for an organization to tailor controls up or down from the *Initial Baseline.*

There is a four-step process to selecting and tailoring a system's *Mission-Adjusted Baseline* as part of Security Control Selection. The steps are:

1. Develop Baseline
    - Define the *Initial Baseline* based upon the FIPS 199 *System Categorization.*
    - Tailor the *Initial Baseline* to create the system's *Mission-Adjusted Baseline* using justification from the OIS;
2. Document
    - Document all baseline decisions; and
3. Obtain approvals for Mission-Adjusted Baselines from the AO and/or the Senior Contractor Official Accountable for Cyber in accordance with the CAS.

For a graphical representation of the procedures described below, see Appendix B, *Control Selection and Tailoring Process.*

To determine the *Initial Baseline*, the organization selects one of three sets of baseline security controls from NIST SP 800-53 Revision 3[8] Appendix E corresponding to the *System Categorization.* This *Initial Baseline* should be documented in the appropriate System Security Plan. Based upon local risk assessment activities, an organization may wish to identify additional controls to supplement the mission specific initial baseline.

[8] Many NIST SP 800-53 controls require organizationally-defined parameters in order to be fully defined.

4.4.1 Tailor the Initial Baseline to develop the Mission-Adjusted Minimum Security Baseline

The overall system categorization, and subsequently the *Initial Baseline* of controls, will already have incorporated a consolidated assessment of impact based upon the correlation of the Organizational Impact Assessment and the local risk assessment with guidance from NIST SP 800-60. However, further tailoring of specific controls in the *Initial Baseline* to develop the *Mission-Adjusted Baseline* enhances an organization's flexibility to determine the baseline set of security controls best suited to their environment, mission, and risk tolerance. The high watermark is used to determine the system categorization and the *initial* baseline set of controls, to achieve a cost-effective, risk-based approach to providing adequate information security organization-wide, organizations should appropriately modify and more closely align controls with specific conditions and/or business functions within the organization.

Tailoring the initial baseline differs from the control deviation process (see Section 4.5.4 Control Deviations). Tailoring is applied to the *Initial Baseline* of controls and is the process by which the *Mission-Adjusted Baseline* is created. Tailoring involves evaluation of the *Initial Baseline* to determine if the baseline mitigates risk commensurate with business need and mission objectives. Control deviation is applied to the *Mission-Adjusted Minimum Security Baseline* and is the process by which control deviations are determined and documented as final adjusted critical controls. Control deviation involves evaluation of the *Mission-Adjusted Minimum Security Baseline* to determine appropriateness and adequacy of each control.

4.4.1.1 Tailoring Security Controls

Based upon the Organizational Impact Assessment, risk assessment, and other requirements, organizations may upgrade, downgrade, or supplement security controls from minimum baselines that resulted from the FIPS 199 *System Categorization* process. Upgrades may occur when the Organizational Impact Assessment determines that the system's mission/business function(s) requires increased risk mitigation beyond the minimum controls defined in NIST SP 800-53 Revision 3 and CNSS 1253. Downgrades may occur when the Organizational Impact Assessment determines that the system's mission/business function(s) does not require the level of protection defined in the initial baseline. Based on risk analysis, specific threats, or external requirements, the control baseline may be supplemented to address residual risks not adequately mitigated by the initial baseline.

4.4.1.2 Tailoring: Downgrades

Consistent with the scoping guidance provided by NIST SP 800-53 Revision 3, control downgrades or the determination to move to a lower baseline may only be considered where: (i) the downgrading action does not affect security objectives other than the objectives targeted for downgrading; (ii) the downgrade is supported by the Organizational Impact Assessment; and (iii) does not adversely affect the level of protection for the security-relevant information within the information system. Downgrade justifications for each downgraded control must be documented in the relevant SSP, risk assessment, or in a stand-alone document.

For additional scoping guidance, see NIST SP 800-53 Revision 3, Chapter 3[9] for unclassified systems, and CNSS 1253, Chapter 3 for NSS.

Additionally, only non-critical controls in the moderate and high baselines can be downgraded. All applicable critical controls from the appropriate *Initial Baseline* must be included in the *Mission-Adjusted Baseline*; organizations may use the control evaluation and deviation process described in *Appendix C: Control Evaluation Process* to evaluate the business impact and implementation of critical controls. Deviation from the baseline controls are customized or tailored to the organizations environment. Once established, this deviation becomes the IA baseline which is validated and continuously monitored.

For NSS, CNSSI 1253, Appendix J defines values for the "*organization-defined*" variables for selected controls. These controls cannot be downgraded or eliminated at this step in the process, but require a documented deviation for equivalencies or exemption (see Section 4.5.4 Control Deviations).

Exhibit 5 below, *Tailoring: Downgrade Eligibility*, depicts which controls care eligible for scoping downgrades based on classification, control type, and baseline.

Classification	Control Type	Baseline	Downgrade Eligibility
NSS	All	All	Not eligible for downgrade
Unclassified	Critical	All	Not eligible for downgrade
Unclassified	Non-Critical	High	Not eligible for downgrade
Unclassified	Non-Critical	Moderate	Eligible for downgrade
Unclassified	Non-Critical	Low	Eligible for downgrade

Exhibit 5: Tailoring: Downgrade Eligibility

4.4.1.3 Common Controls

Common controls are security controls that are inherited by one or more information systems within the organization. Common controls should be evaluated by the organization relying on them to ensure they implement an adequate level of security for the system. In cases where the control is insufficient based on the needs of the system, the system owner must supplement the control with system-specific or hybrid controls. For NSS, common controls should consider CNSS 1253 and DOE directives on physical and telecommunications security.

[9] The following security controls are recommended candidates for downgrading: (i) confidentiality [MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) integrity [SC-8]; and (iii) availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE- 11, PE-13, PE-15, SC-6].

4.4.2 Document the Mission-Adjusted Minimum Security Baseline

The resulting set of security controls along with the supporting rationale for selection decisions represents the system's *Mission-Adjusted Baseline*. Organizations must document the decisions taken during the Under Secretary of Energy Control Tailoring Process, providing a sound rationale for those decisions. This documentation is essential when examining the security considerations for information systems with respect to potential mission/business impact. The new *Mission-Adjusted Baseline* and supporting documentation must be included in the appropriate System Security Plan (SSP), including any significant risk management decisions in the security control selection process.

4.5 Security Controls Implementation

This step aligns with Step 3 of the RMA, *Implement Security Controls,* as well Step 4, *Assess Security Controls.* Once the *Mission-Adjusted Baseline* has been selected, an evaluation of (1) the risk addressed by the control, and (2) the potential business impact of implementing the control to address the identified risk, should take place. This evaluation of risk mitigation and business impact will help determine the appropriate implementation for each control. See *Appendix C: Control Evaluation Process* for guidance on evaluating controls.

4.5.1 Program Management Controls

NIST SP 800-53 Revision 3 includes a new control family, Program Management (PM). The PM controls focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. The Office of the CIO and the Office of the Under Secretary Cyber Security Program implements many of these controls, which can be inherit by the organizations within the Office of the Under Secretary of Energy. Exhibit 6 below, *Implementation of Program Management Controls*, describes the implementation of each control within DOE. An implementation status for all PM controls must be included in applicable SSPs.

Control Identifier	Control Title	DOE Implementation	Inherited (Y/N)
PM-1	Information Security Program Plan	The Energy Programs RMA IP fulfills this control.	Yes
PM-2	Senior Information Security Officer	DOE has appointed a Chief Information Security Officer for the Department.	Yes
PM-3	Information Security Resources	The OCIO maintains a capital planning program to manage the Department's resources.	Yes
PM-4	Plan of Action and Milestones Process	The OCIO collects and reports POA&Ms on a quarterly basis via a defined, structured process.	Yes
PM-5	Information System Inventory	The OCIO collects and reports system inventories on a quarterly basis via a structured process.	Yes
PM-6	Information Security Measures	Organizations shall develop appropriate performance metrics. NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security* provides guidance for the development of appropriate performance metrics	No
PM-7	Enterprise Architecture (EA)	The OCIO maintains EA support for all Departmental elements.	Yes
PM-8	Critical Infrastructure Plan	This control is not applicable to organizations that do not have critical infrastructure.	No
PM-9	Risk Management Strategy	The Department's RMA satisfies this control.	Yes
PM-10	Security Authorization Process	The Energy Programs RMA IP implements this control.	Yes
PM-11	Mission/Business Process Definition	The Organization Impact Statement implements this control.	No

Exhibit 6: Implementation of Program Management Controls

4.5.2 Under Secretary of Energy Initial Baseline Critical Controls

The Under Secretary of Energy Baseline Critical Controls are provided as an initial set of suggested critical controls to evaluate, and are based on the SANS Institute twenty (20) "specific technical security controls that are viewed as effective in blocking currently known high-priority attacks, as well as those attack types expected in the near future." This list of 20 critical control areas, called the SANS Consensus Audit Guidelines (CAG), provides a prioritized baseline of information security control areas that can be used as a focus for continuous monitoring for unclassified systems. This CAG baseline and its correlating list of NIST SP 800-53 security controls make up the Under Secretary of Energy Initial Baseline Critical Controls. The Office of the Under Secretary of Energy, as well as Program Offices and sites may consider additional controls critical based on persistent threats or other factors.

4.5.3 Mission-Adjusted Baseline Critical Controls

Appendix E: *Under Secretary of Energy Baseline Critical Controls* lists the SANS CAG control areas and maps these areas to approximately 125 NIST SP 800-53 controls. Under Secretary of Energy organizations have the flexibility to use a risk based approach to selecting critical controls from this baseline, and establishing a tailored list of controls that will be considered "critical" for each system or organization. This list is referred to as the Mission-Adjusted Baseline Critical Controls. The process for adjusting critical controls is similar to the process for adjusting controls from the initial baseline as described in section 4.4.

At a minimum, Under Secretary organizations must ensure their mission-adjusted critical controls:

- Take into account the OIS, including considering whether controls not identified in the CAG should be added based on risk;
- Are adequate to provide the appropriate assurance level for continuous monitoring activities to include appropriate decision support for annual system authorization by the AO; and
- Support performance measurement and assurance objectives.

Since organizations are encouraged to select their critical controls based on risk, deviations for critical controls are expected to be requested only in rare circumstances. Note that deviations for critical controls are only applicable to those critical controls and/or enhancements present within the *Mission -Adjusted Minimum Security Baseline*. It is possible for one or more of these controls to be absent from a system's baseline based upon the system's categorization.

The process described below is expected to apply to unclassified systems for all Under Secretary organizations, including those with M&O contracts, unless otherwise described by the system authorization process in the CAS (for M&O contracts only).

The high level-process for determining critical controls is as follows:

- **Step 1:** Begin with the Under Secretary of Energy Initial baseline Critical Controls as described in Appendix E, *Under Secretary of Energy Baseline Critical Controls*;
- **Step 2:** Remove any NIST SP 800-53 controls that are not part of the system's Mission-Adjusted baseline;
- **Step 3:** Evaluate remaining controls based on risk and ensure the controls selected support continuous monitoring (including decision support for annual system authorization), performance;
- **Step 4:** Determine if addition controls are needed based on the OIS;
- **Step 5:** Document justifications for changes to CAG (including additions) as expressed in Appendix E, *Under Secretary of Energy Baseline Critical Controls*; and
- **Step 6:** Document the final adjusted critical controls in the relevant SSP, Continuous Monitoring Plan, or in a stand-alone document.

Note: Critical controls for NSS are defined by the site, based on assessment of risks, and are not based on the SANS CAG.

4.5.4 Control Deviations

Based upon the control evaluation described in Appendix C: *Control Evaluation Process*, Under Secretary organizations have the flexibility to deviate from the *Mission-Adjusted Minimum Security Baseline*. Requests for such deviations must follow the process outlined in paragraph 6.a.(3) (c) of DOE O 251.1C and are further described below.

Control deviation differs from the process of tailoring the initial baseline (see Section 4.4.1 Tailor the Initial Baseline). Control deviation is applied to the *Mission-Adjusted Minimum Security Baseline* and is the process by which control deviations are determined and documented as final adjusted critical controls. Control deviation involves evaluation of the *Mission-Adjusted Minimum Security Baseline* to determine appropriateness and adequacy of each control. Tailoring is applied to the *Initial Baseline* of controls and is the process by which the *Mission-Adjusted Baseline* is created. Tailoring involves evaluation of the *Initial Baseline* to determine if the baseline mitigates risk commensurate with business need and mission objectives.

The RMA defines two possible deviations from control requirements defined by NIST: (1) an *equivalency* or (2) an *exemption.*

- **Equivalencies** are approved conditions that technically differ from a control requirement but provide equivalent protections or compensatory measures to mitigate risk to an acceptable level.

All *equivalencies* must be documented in the relevant SSP, risk assessment, or in a stand-alone document. Equivalencies must be approved by the AO, or in accordance with the authorization process documented in the CAS for M&O contracts. In addition, equivalencies for NSS must be documented in the risk assessment. The AO may approve equivalencies by granting a system authorization, contingent upon the equivalencies being formally identified in the SSP.

- **Exemptions** are approved deviations from a control requirement for which *no compensatory measures or alternative controls are implemented* resulting in an unmitigated risk. Exemptions should be approved only when compensatory measures cannot be implemented or correction of the condition is neither feasible nor cost-effective.

All *exemptions* must be documented in the relevant SSP, risk assessment, or in a stand-alone document. Exemptions must be approved by the AO, or in accordance with the authorization process documented in the CAS for M&O contracts. In addition, exemptions for NSS must be documented in the risk assessment. Additional documentation requirements exist depending on the system categorization and the criticality of the control.

- Exemptions for ***critical controls*** for unclassified systems:
  - For moderate and high systems, critical control exemptions must be formally documented. Once approved, a copy of the documentation must be **provided** to the Office of the Under Secretary.
  - For low systems, critical control exemptions must be formally documented. A copy of the documentation must be **available** to the Office of the Under Secretary of Energy upon request.
- Exemptions for ***non-critical controls in low, moderate, or high unclassified systems*** should be formally documented and made available to the Under Secretary of Energy's Office upon request.
- For NSS, copies of documented exemptions should be available for review onsite by the Under Secretary of Energy's Office based on appropriate clearances and need to know.
- All control exemptions for both unclassified systems and NSS must be re-evaluated for validity at least annually, or if a security significant change occurs within the system.

All control deviations (equivalencies and exemptions) must be re-evaluated for validity at the end of the system's authorization period, or if a security significant change occurs within the system.

See **Error! Reference source not found.** for a graphical representation of this process.

4.5.5 Organization-Defined Parameters and Specified Requirements

4.5.5.1 Organization-Defined Parameters

Security controls containing organization-defined variables or parameters (e.g., actions, percentages, frequency, time periods, etc.) provide organizations with the flexibility to customize specific controls (1) to support explicit organizational requirements and objectives, and (2) to best protect resources within the context of the operational and technical environment.

The values of organization-defined variables should be based upon risk, best practice, and technical effectiveness, and can be defined at the Department, program, site, or system level. At the Department, program, or site level, definition of these values can be provided via management direction, policies, contracts, etc., and the required parameters will propagate hierarchically through established management or operational channels. At the system level, if the value is not explicitly inherited from the Department, program, site, or subsuming system, values should be assigned (1) after the control tailoring process and definition of the mission-adjusted baseline, and (2) during to the control implementation and/or deviation process.

Once established, values for organization-defined parameters must be adhered to unless more restrictive values are required to address specific program, site, or system risks. These more restrictive values should be documented in the SSP with supporting information. Deviations from organization-defined parameters that would likely lessen a control's security effectiveness should be based upon solid risk management principles and follow the control deviation process defined in the RMA.

For NSSs, guidance for determining organization-defined variables is provided in CNSS 1253. Appendix J of CNSS 1253 establishes specific values for organization-defined parameters common to NSSs. Listed in table form are specific values (or ranges of values) for those security controls (or control enhancements) for all NIST SP 800-53 Revision 3 controls. Some organization-defined parameters in Appendix J have no values listed. For those control parameters, common ranges of values are not required across NSS, and organizations should define the associated values based on CNSS 1253 guidance.

Approval of all organization-defined parameters, like all control safeguards, rests with the AO and/or according to the documented authorization process in the CAS for M&O contracts); all organization-defined variables will be part of the controls defined in the mission-adjusted baseline, documented in the SSP, tested in accordance with the test plan, assessed based on the results of the test plan, subsequent residual risk documented in the security assessment report (SAR), and monitored within the continuous monitoring strategy and plan.

4.5.5.2 DOE Specified Requirements

The US DOE O 205.1B provides specific requirements supporting the security posture and operation of classified and unclassified systems. These requirements incorporate application of a number of cyber security control areas. The following list contains security requirements and associated order references:

System use notification (e.g., warning banner) for unclassified systems (4.c.(11))
Risk-based protection of media (4.c.(12))
Information marking for unclassified systems (4.c.(14))
Information marking for NSS (4.c.(15))
Security and risk management of NSS (4.c.(16))
Electronic media sanitization and disposal for NSS (4.c.(17))
NSS requirements for RD, FRD, and TFNI (4.c.(19))

4.6 Information System Authorization

This step aligns with Step 5 of the RMA, *Authorize Information Systems.* As required by OMB Circular A-130[10], Appendix III, federal information systems must (1) obtain in writing an authorization to operate (ATO) and (2) be reauthorized within designated control assessment cycle or upon significant change. The AO for a system will review the system's authorization package to determine whether to provide this written ATO. This authorization package will include at a minimum:

- Risk Assessment (RA)
- System Security Plan (SSP)
- Security Assessment Report (SAR) [11]
- Plan of Actions and Milestones (POA&M)
- Privacy Impact Assessment (PIA)
- Configuration Management Plan
- Contingency Plan
- Continuous Monitoring Plan
- Authorization Letter

The above documentation is not static, and should be updated continuously based on situational awareness, such as the introduction of new threats, self and independent assessments, and the status of vulnerability remediation for example. Additional guidance on authorization and the development of required documentation is provided in NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. A system's ATO will remain in effect until a reauthorization is required. Reauthorizations may be *time-driven* or *event-driven* and should be part of a comprehensive continuous monitoring strategy as discussed in the following section.

[10] http://www.whitehouse.gov/omb/circulars_a130_a130trans4

[11] The SAR should include the testing methodology used and the test results; otherwise that information must be provided as standalone documents (e.g. Test Plans, Test Results).

4.7 Continuous Monitoring Strategy

Pursuant to best practices, OMB and NIST guidance, the Office of the Under Secretary of Energy encourages an emphasis on continuous monitoring of information systems. The Office of the Under Secretary of Energy recognizes that government and information security industry thought leaders have acknowledged that there are deficiencies and security gaps associated with the security authorization process, or in particular how it has been typically implemented as a "paperwork" process without robust continuous monitoring. Since systems and threats aren't static, security authorization and continuous monitoring approaches must also be iterative processes. The approach described in this section is built on lessons learned, and shifts the emphasis to processes that support on-going decision making. The annual system authorization process described moves Under Secretary organizations closer to "real time" system monitoring. The evolution of this process is depicted in Exhibit 7 below, *Notional System Authorization Evolution Process*.

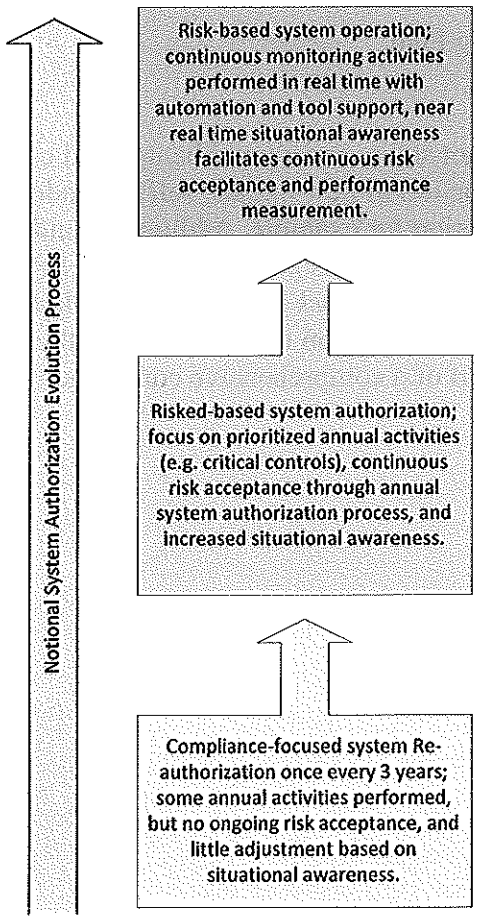


Exhibit 7: Notional System Authorization Evolution Process

This step aligns with Step 6 of the RMA, *Monitor Security Controls*. An effective continuous monitoring strategy will (1) manage the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment; (2) provide organizations with an effective mechanism to update security plans, security assessment reports,

and plans of action and milestones; and (3) ensure the continuous assessment and acceptance of residual risk throughout the system lifecycle. The continuous monitoring strategy includes the five components listed below. Each organization must document a continuous monitoring plan consistent with this strategy (RMA Step 6). Guidance for establishing a continuous monitoring plan can be found in NIST SP 800-53 Revision 3 and NIST SP 800-37 Revision 1.

1. Configuration management and control processes for organizational information systems.
    a. Security impact analyses on actual or proposed changes to organizational information systems and environments of operation.
    b. Assessment of SSC.
2. Assessment of selected security controls (including system-specific, hybrid, and common controls).
    a. All critical control areas present within the mission-adjusted baseline must be assessed annually.
    b. A subset of the remaining, non-critical controls should be assessed on an annual basis.
    c. All controls within the mission-adjusted baseline must be assessed within a system's control assessment cycle as (3 years for unclassified Low systems, 4 years for unclassified Moderate systems, 5 years for unclassified High systems, unspecified for NSS)
    d. Assessment results should be formally documented and made available for review upon request.
3. Security status reporting to appropriate organizational officials.
    a. The AO must be notified of planned security significant changes, or of other increases to system risk, prior to implementation.
    b. The AO must be notified of any unapproved security significant changes or increases to residual risk that may have resulted from maintenance activities, environmental changes, or system events.
    c. The AO will determine whether a SSC warrants a re-accreditation, or if further action is required.
    d. The AO should be informed at least quarterly of new identified weaknesses, the status of POA&M item resolution, and any other information relevant to ongoing security and risk management. For NSS, security status reporting must be conducted in accordance with DOE O 470.4-1, Chg.1, section N.
    e. System documentation (RA, SAR, SSP, and POA&M) should be continually maintained and updated, with a summary of changes presented to the AO no less than annually.
4. Active involvement by the AO in the ongoing management of information system-related security risks.
    a. Based upon the implementation and maintenance of the continuous monitoring strategy, and review of applicable security documentation, the AO must assess and approve the continued authorization of a system at least annually. This strategy aligns the continuous monitoring program with the concept of continuous system authorization with as close to "real time" monitoring as is practical.

b. This annual acceptance of residual risk and approval of the continued authorization must be documented and available for review upon request.

5. Active monitoring of current and evolving threats to assess changes to the system risk profile.

Continuous monitoring for M&O contracts is expected to align with the process described above, but will be accomplished via the mechanism described in the CAS. The AO and the Senior Contractor Official Responsible for Cyber are responsible for establishing and understanding the terms of the CAS as it relates to continuous monitoring, including any reporting or notification requirements. At a minimum, the process will include annual acceptance of residual risk by the AO as described in Step 4 above.

4.7.1 Time-Driven Reauthorizations

Time-driven reauthorizations occur when a system's control assessment cycle has expired. The control assessment cycle is the time period by which 100% of documented controls must be tested. The requirements for control assessment based on system sensitivity and classification are listed in Exhibit 8: *Time-based Authorizations and Control Assessments*

In summary:

- Control assessment cycles are defined as:
  - 5 years for unclassified Low systems
  - 4 years for unclassified Moderate systems
  - 3 years for unclassified High systems
  - Unspecified for NSS
- Critical controls for Moderate and High unclassified systems must be independently assessed annually at least once during the control assessment, independence is defined in section 2.3 of this document, *Assessments*.
  - If the security control assessments are conducted by Security Control Assessors with the required degree of independence, the assessment results can be cumulatively applied to the reauthorization, thus supporting the concept of ongoing authorization. For example, the reauthorization action can be as simple as updating critical security status information in the authorization package (i.e., the security plan, security assessment report, and plan of action and milestones) and obtaining AO approval and signature for the updated authorization decision document based on the current determination and acceptance of risk.
- A subset of non-critical controls within the mission-adjusted baseline, should be assessed regularly (e.g., monthly, quarterly or annually) and each control must be assessed at least once within each control assessment cycle.
- Non-critical controls within the mission-adjusted baseline require no independent assessment.
- The authorization periods listed below include an annual assessment by the AO of residual risk and approval for the continued authorization of the information system, as a part of the continuous monitoring strategy.
- Time-driven authorizations for M&O contracts will be accomplished in accordance with the system authorization process described in the CAS.

	Unclassified Low	Unclassified Moderate	Unclassified High	NSS
Critical Controls	• Self-assessment of each critical control at least annually	• Independent[12] security testing and evaluation (ST&E) of each critical control at least once every 4 years • Self-assessment at least annually	• Independent ST&E of each critical control at least once every 3 years • Self-assessment at least annually	*
Non-Critical Controls	• Self-assessment of each control at least once every 5 years	• Self-assessment of each control at least once every 4 years	• Self-assessment of each control at least once every 3 years	*
All Systems	Documented annual residual risk assessment, approved by the AO and available for review by the Office of the Under Secretary of Energy.			

* Due to data sensitivity and a "need to know", the level of assessments is to be determined by the organization.

Exhibit 8: Time-based Authorizations and Control Assessments

4.7.2 Event-Driven Reauthorizations

Any instance of change to the fundamental aspects of system risk, or to the risk management process upon which the original risk assessment was conducted, and on which the corresponding authorization was granted, is considered a Security Significant Change (SSC). The AO will determine whether a SSC warrants a re-accreditation, or if further action is required.

12 The level of independence required for ST&E should be determined by the Authorizing Official , as described in Section 2.3 of this document.

Triggers that may indicate a SSC include, but are not limited to the following:

- Introduction of a new technology that has the potential to alter the fundamental system residual risk or to introduce unmitigated system vulnerability; (e.g. introduction of a new operating system or a new wireless access capability),
- Discovery of significant, previously-unmanaged vulnerabilities;
- Significant change in the threat basis (e.g. new threat source or change in threat likelihood);
- Introduction of new data type with the potential to change the system security categorization or consequence of loss (CoL) (e.g. data and system characterization and corresponding impact levels);
- Increase in system vulnerability due to lack of mitigation capabilities (e.g. impediments to system security patching);
- Change in mission function or political landscape that could alter subsequent risk tolerance;
- New or planned system interconnections; and
- Change to the contractor who manages, maintains, or operates the system.

In general, routine maintenance, additional instances of identical approved assets/security configurations, and general approved patching do not constitute an SSC. The assessment of change to system risk, and the subsequent determination of SSC, should be incorporated into an organization's change control, configuration management, and continuous monitoring processes and procedures.

Following the assessment of a triggering event, a written summary of all SSCs should be provided to the Authorizing Official for review and approval prior to implementation and/or upon immediate upon. Note that comprehensive change management processes should trigger and be integrated with SSC processes.

For M&O contracts, SSC determination will be agreed upon and documented as part of the system authorization process described in the CAS. At a minimum, the CAS security authorization process will describe what is considered a SSC, and the process once an SSC occurs.

5 Threat Management

The ability to maintain an acceptable cyber security posture for the Energy Program Offices is dependent on awareness of current threats and effective vulnerability incident management processes. It is important for senior management to understand the components and sequence of activities that make up an effective incident response program. Likewise, it is just as important for cyber security leaders to understand their Programs' missions in order to correlate security risks and threats with business objectives.

5.1 Key Concepts

FIPS 200 defines threat, vulnerability, and risk as:

- **Threat** - *Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.*

- **Vulnerability** - *Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.*

- **Risk** - *The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.*

The equation fundamental to determining the relationship of these concepts is as follows:

Risk = Threat x Vulnerability x Impact (consequence)

5.2 Threat Awareness and Response

All validated cyber security incidents involving Federal information or Federal information systems, including privacy breaches, under DOE or DOE contractor control must be identified, mitigated, categorized, and reported to the DOE Joint Cybersecurity Coordination Center (JC3-CIRC) in accordance with JC3-CIRC procedures and guidance[13].

JC3-CIRC issues advisories that describe new vulnerabilities in information systems and provide information on mitigating the vulnerabilities. Promptly releasing such information is a high priority because of the direct link between vulnerabilities and incidents.

Distributing information about current incidents also assists Energy Program Offices in identifying signs of such incidents.

Energy Program Offices must maintain awareness of current security threats and be able to consistently demonstrate:

- Receipt of JC3-CIRC advisories;
- Analysis of prioritized advisories for applicability to an Energy Program Office or site;
- Action taken to mitigate high risks and minimize the threat or impact of an incident based on JC3-CIRC advisories;
- Reporting metrics of averted or minimized impact to business operations due to proactive response to threats; and a consistent method of keeping the AO and mission owners apprised of threats.

[13] http://www.doecirc.energy.gov/incidentreporting.html

Cyber security incidents involving NSS must be reported in accordance with the requirements in DOE M 470.4-1, chg.1, *Safeguards and Security Program Planning and Management*. If loss or unauthorized disclosure of classified information associated with NSS is suspected, the incident must be immediately reported to the AO. In addition, the Energy CSPM is to be notified of all high security incidents.

NOTE: Additional notification requirements for incidents involving the compromise of personally identifiable information can be found in DOE Order 206.1, *Department of Energy Privacy Program.*

6 Security in the System Development Lifecycle

An effective Risk Management approach must be integrated into the DOE's System Development Lifecycle (SDLC) to minimize negative impact on the mission and organization. This section of the Energy Implementation Plan provides explanation for the integration of the five phases of the IT SDLC; Initiation, Development or Acquisition, Implementation, Operation or Maintenance, and Disposal. The following subsections elaborate on each phase displayed in Exhibit 9 below, *Integration of Risk Management into the SDLC.*

SDLC Phases Phase	Characteristics Support from Risk	Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment (ecisions regarding risks identified must be made prior to system operation)
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies and procedures.	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational production environment (e.g. new system interfaces)

SDLC Phases Phase	Characteristics Support from Risk	Management Activities
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software.	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

Exhibit 9: Integration of Risk Management into the SDLC

6.1 System Initiation

The first phase of the system development lifecycle (SDLC) provides activities related to the initiation of system development activities. This phase relies heavily on the collaboration between those within the organization who ensure that mission needs are met and the underlying supporting systems supporting those mission needs, and the technical staff responsible for implementing and maintaining those mission-focused systems.

General activities for this phase include:

- Determining whether activities are consistent with the organizational IT Strategic Plan, mission objectives, and budgetary constraint
- Assessing business cases
- Assessing consistency with target architecture
- Beginning the risk management process

Cyber security activities for this phase include:

- Initial system categorization
- Determining high level security and privacy requirements

6.2 System Development/Acquisition

In the second phase of the SDLC, the system is designed and system components are acquired. It is during this phase that functional, security, and integration requirements are communicated to solution providers.

General activities of this phase of the SDLC include:

- Ensuring system design is consistent with architecture standards
- Identifying integration issues with other systems and shared services

Cyber security activities for this phase include:

- Assessing risk
- Designing the security architecture
- Functional and security testing

6.3 System Implementation

During this phase the newly developed system is placed in the production environment. Here, the outcomes of the security assessments are managed and residual risks are identified as the system is prepared for implementation.

General activities of this phase of the SDLC include:

- Integrating the system into the environment
- Confirming that the functional requirements are met

Cyber security activities for this phase include:

- Finalize system categorization
- Implement protective measures to address security and privacy requirements
- System authorization

6.4 System Operation and Maintenance

This phase of the SDLC deals with the activities for continuing to operate and maintain the information system. It requires periodic assessments of security, functionality, and business processes.

General activities of this phase of the SDLC include:

- Defining change drivers and business and information management requests
- Managing the enterprise architecture
- Evaluating performance, efficiency, redundancy, and risk

Cyber security activities for this phase include:

- Managing configuration and security impact of changes
- Continuous monitoring
- Evaluating ever-changing threats

6.5 System Disposal

The final phase of the SDLC provides for the disposal of a system's constituent components, close-out of contracts, transfer of data to other organizations, sanitization of assets, etc. It is a collaborative process with technical staff and management, the cognizant Enterprise Architecture capability, records personnel, property management, and others. DOE G 200.1-1 Appendix F, *Computer System Retirement Guidelines* provides guidance on initiating the process to "retire" a

system. NIST SP 800-64 Revision 2, *Security Considerations in the SDLC* provides additional guidance on system disposition as well.

Once a system is specified to be retired, three major issues must be addressed: (1) information and system security, (2) data preservation and/or transfer, and (3) regulatory compliance. The system owners have the responsibility to coordinate with operations staff, the AO, and others to address these cyber security considerations.

Due to the interconnected nature of systems, the persistent threat of attacks, insider threats, improper data exfiltration, etc., it is imperative that a system disposal plan be developed. Such a plan should explicitly address security concerns throughout the disposal phase of the system's lifecycle. This plan should provide retirement details for all subsystems and/or system inventory, with milestones and schedule dates by which these assets will (1) be removed from production, (2) have their data transferred/archived, and (3) be sanitized[14] and disposed (via destruction, transfer, gifting, etc.). This will ensure a prioritized, holistic approach to system shut down.

Data preservation needs will be driven by records requirements, programmatic retention requirements, and legal requirements. In addition, operational security will need to be maintained throughout the disposition phase. To ensure that these requirements are met, and any necessary functionality preserved, the disposition/disposal plan must address all aspects of the last phase of the SDLC. The plan should include:

- Assurance of continued security monitoring, patching, vulnerability scanning, etc., Provide explicit details where necessary, such as maintaining perimeter and host controls until all data is removed from production.
- Security controls and/or processes that may be associated with system disposition should be detailed and tested/assessed to ensure efficacy (e.g., account termination, physical controls, incident reporting, and sanitization).
- Update or termination of applicable Privacy Impact Assessments (PIAs) pursuant to DOE O 206.1, *DOE Privacy Program.*
- Collaboration with stakeholders concerning interconnections, inherited controls, shared hardware, and/or shared risk to facilitate management of their risks and to coordinate transfer of control of their assets accordingly.
- Data preservation methodology, format, and encryption level.

If data and/or system components are going to be transferred to another organization, the receiving organization should provide input in the development of the disposition plan. The receiving organization's requirements and/or risk tolerance will determine the required data format(s), encryption levels, and sanitization methods applicable to the transferring components.

[14] Sanitization requirements are explicitly detailed by Federal and Departmental policy and NIST SP 800-88, *Guidelines for Media Sanitization.*

The System Owner should present the disposal plan to the cognizant AO as a supplement to the System Security Plan, accompanied by a letter indicating a security significant change. Upon review of the proposed change(s) and the attached disposition plan, the AO can evaluate risk and determine the system's authorization status throughout disposal.

Once the disposal plan is approved by the AO, executed, and completed, an assessment must to take place to determine any outstanding system issues and to provide a final closure to the AO and the Under Secretary of Energy CSPM. At this point, the system can be removed from the Departmental FISMA inventory, and a notification can be provided to the OCIO. Coordination must also take place with the capital planning staff to ensure any closure requirements occur for related IT investments.

7 Contractor Assurance System

DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, and in particular the associated Contractor Requirements Document (Attachment 1), sets forth policy requirements for DOE contractors to implement a CAS. The CAS may be developed by M&O contractors if desired, and will be submitted to site offices for acceptance. For established M&O contracts, the nine CAS areas referenced below may be mapped to existing mechanisms as appropriate, so long as the existing mechanism implements the requirement described, and a requirements mapping is performed and documented.

In coordination with DOE laboratories and organizations with oversight responsibilities, the Under Secretary of Energy implements the requirements by ensuring that any CAS addresses, at a minimum, the following nine areas:

No.	Area	Description
1	**Program/Mission Support for Cyber**	• Define and describe how senior officials with an understanding of program and mission risk will be integrated into cyber processes to ensure organizational risk is managed adequately and in accordance with program and mission risk.
2	**Change Management**	• Define and describe general strategies for change management to the CAS itself, or operational processes, procedures, roles, etc. defined within the CAS; • Implement a change management process that defines how senior contract officials will interact and communicate change management issues with Federal counterparts.

No.	Area	Description
3	**Risk Profile Definition, Management, and Performance**	• Define the risk profile for systems; • Implement processes and procedures for active monitoring of changing environments and evolving threats; • Define how those processes will impact the risk profile, and how changes will be managed, approved and communicated (including roles and responsibilities); and • Implement metrics and techniques for measuring performance in support of risk profile management.
4	**Performance Management, Accountability and Transparency**	• In coordination with contracting officials, formally document and define contractor performance expectations, how they will be measured, tracked and communicated; • Implement a documented strategy regarding transparency into operations by DOE Federal authorities to include reporting frequency, process and level of detail; and • Formally document the consequences of missing performance targets or reporting requirements.
5	**Lessons Learned**	• Define strategies and processes for providing internal continuous feedback of lessons learned; and • Define methods and processes for sharing lessons learned outside of the organization with other Under Secretary of Energy Programs.
6	**Awareness and Training (Human Performance)**	• Define an overall strategy for awareness and training; • Determine audiences, frequencies and methods for delivery; • Design and manage systems to track completed training; and • Determine strategies for measuring the impact of training on individual performance, and how to continuously improve training quality and effectiveness based on performance.
7	**System Authorization Process**	• Define and document processes and procedures for managing system authorization; and • Define and document how the Senior Contractor Official Responsible for Cyber will interact with Authorizing Officials and other Federal employees and stakeholders.
8	**Contingency Planning/ Disaster Recovery**	• Define objectives (e.g. maximum allowable outage), processes and procedures for ensuring data recovery and reconstitution according to a documented strategy.

No.	Area	Description
9	**Incident Response**	• Implement strategies, processes and procedures for incident response, and in particular how the contractor will interact with JC3-CIRC, US-CERT, and any others as defined; • Document how incidents involving privacy data will be managed; and • Document, in coordination with AOs, how incident and event information will be communicated, reported and shared.

Exhibit 10: Contractor Assurance System Requirements

CAS has been referenced throughout this document, and in particular when processes are expected to be different than standard processes due to increased Federal reliance on contractor systems. All requirements of the Energy Programs RMA IP apply to contractor managed facilities and information systems, unless specifically excluded. Exhibit 11 below, *Contractor Assurance System Reference Table*, maps references to the CAS throughout this document, and is provided for clarification and consolidation of CAS-related discussions.

Section	Section Title	Relevance to CAS
1.2	Scope	The Energy Programs RMA IP applies equally to all Under Secretary entities, except as specifically mentioned throughout this document, and referenced in this table.
2.1	Risk-based Approach to Cyber Security Governance	Performance assurance for M&O contracts is delivered through the Contractor Assurance System model.
2.2.1	Under Secretary of Energy Oversight of Programs	Introduces the CAS as a critical component of Energy's program oversight, and references this section.
2.2.2.1	Performance Metrics	The Under Secretary will implement high-level performance measurement, and the CAS is expected to define more detailed performance measurement, as well as expectations and communication.
2.3	Assessments	Assessment requirements for M&O contracts are described in the CAS System Authorization Process, and must include at a minimum: 1. Type and frequency of required assessments; 2. Acceptable levels of independence, definition of independence (if needed); and 3. Processes required for weakness tracking and remediation.

Section	Section Title	Relevance to CAS
3.8	Senior Contractor Official Accountable for Cyber	Role description for the Senior Contractor Official Accountable for Cyber.
4.4	Development of the Mission-Adjusted Minimum Baseline of Security Controls	CAS defines the authorization process, to include the approval process for mission-adjusted baselines.
4.5.2	Under Secretary of Energy Baseline Critical Controls and Control Adjustment	Process for baseline Critical Control definition unless an alternative process is described by the system authorization process in the CAS.
4.5.3	Control Deviations	Equivalency and exemption procedures must be documented, but may be approved in accordance with the authorization process documented in the CAS for M&O contracts.
4.5.4.1	Organization-Defined Parameters	Approval of all organization-defined parameters is according to the documented authorization process in the CAS for M&O contracts.
4.7	Continuous Monitoring	Continuous monitoring for M&O contracts is expected to align with the principles described in this section, but will be accomplished via the mechanism agreed upon in the CAS including any reporting or notification requirements. *Note: At a minimum, the process will include annual acceptance of residual risk by the AO.*
4.7.1	Time Driven Reauthorizations	Time-driven authorizations for M&O contracts will be accomplished in accordance with the system authorization process described in the CAS.
4.7.2	Event Driven Reauthorizations	Security Significant Change (SSC) for M&O contracts will be defined and documented as part of the CAS. At a minimum, the CAS security authorization process will; • Describe what is considered a SSC; and • Document the process to be followed once an SSC occurs.

Exhibit 2: Contractor Assurance System Reference Table

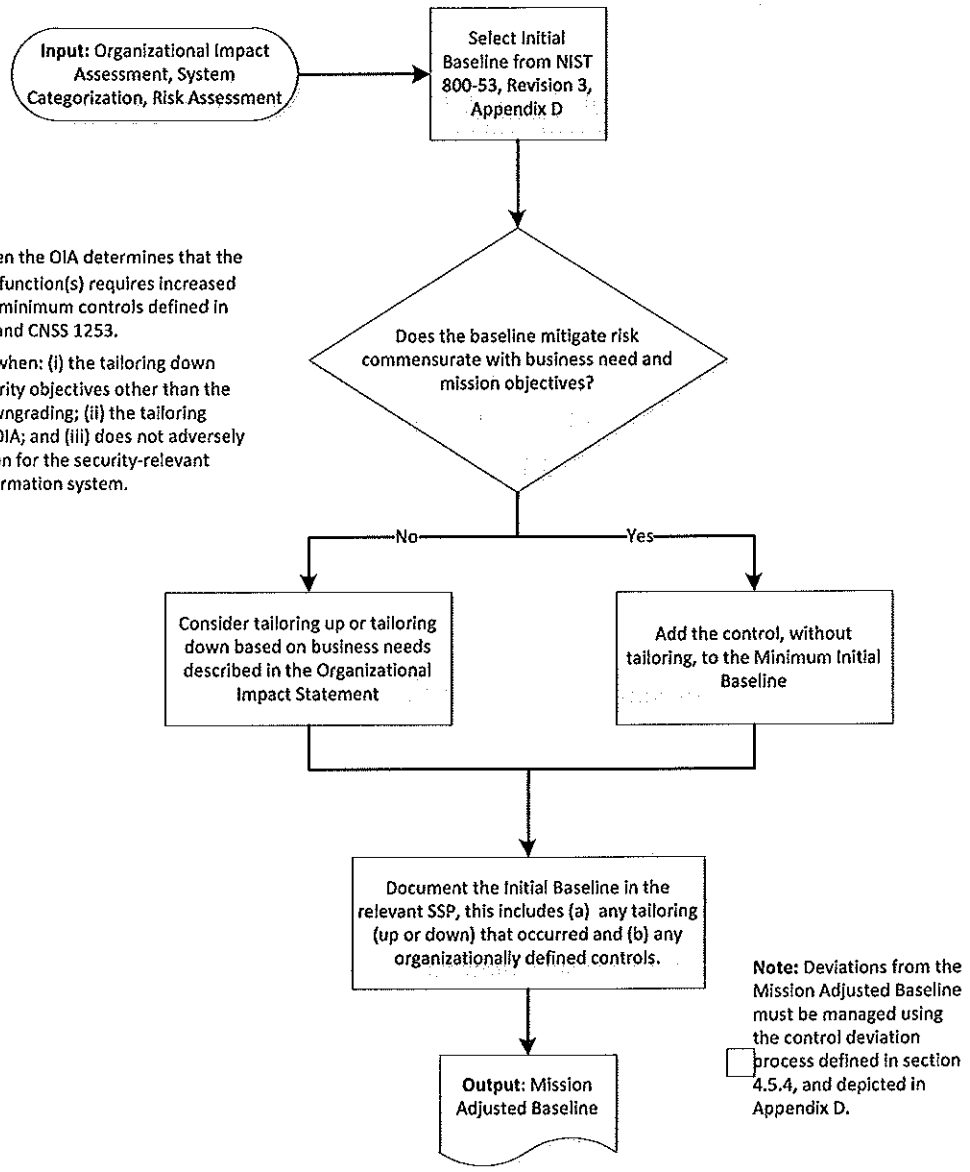
Appendices

Appendix A: Acronym List

Acronym List	
Acronym	Term
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
CFR	Code of Federal Regulations
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CO	Contracting Office
COL	Consequence of Loss
CRD	Contractor Requirements Document
CSPM	Cyber Security Program Management
DART	Departmental Audit Reporting & Tracking System
DNSSEC	Domain Name System Security Extensions
DOE	Department of Energy
DOE O	Department of Energy Order
DOE JC3-CIRC	Department of Energy Joint Cybersecurity Coordination Center
EE	Office of Energy and Office of Electricity
FE	Fossil Energy
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IMGC	Information Management Governance Council
IP	Implementation Plan
IPV6	Internet Protocol Version 6
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology

Acronym List	
Acronym	Term
M&O	Management and Operation
MOU/A	Memorandum of Understanding/Agreement
NE	Nuclear Energy
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSS	National Security System
OCIO	Office of the Chief Information Officer
OE	Electric Delivery and Energy Reliability
OIS	Organizational Impact Statement
PIA	Privacy Impact Assessment
POA&M	Plan of Actions and Milestones
PSO	Program Security Office
PSO	Program Secretarial Offices
Q1	Quarter 1
RA	Risk Assessment
RMA	Risk Management Approach
SANS CAG	SANS Consensus Auditing Guide
SAR	Security Assessment Report
SDLC	System Development Life Cycle
SDM	Security Device Manager
SSC	Security Significant Change
SSP	System Security Plan
TIC	Trusted Internet Connection
WFO	Work for Others

Appendix B: Control Selection and Tailoring Process



Note:

- Tailoring up may occur when the OIA determines that the system's mission/business function(s) requires increased risk mitigation beyond the minimum controls defined in NIST SP 800-53 Revision 3 and CNSS 1253.
- Tailoring down may occur when: (i) the tailoring down action does not affect security objectives other than the objectives targeted for downgrading; (ii) the tailoring down is supported by the OIA; and (iii) does not adversely affect the level of protection for the security-relevant information within the information system.

Exhibit 3: Under Secretary of Energy Control Selection and Tailoring Process

Appendix C: Control Evaluation Process

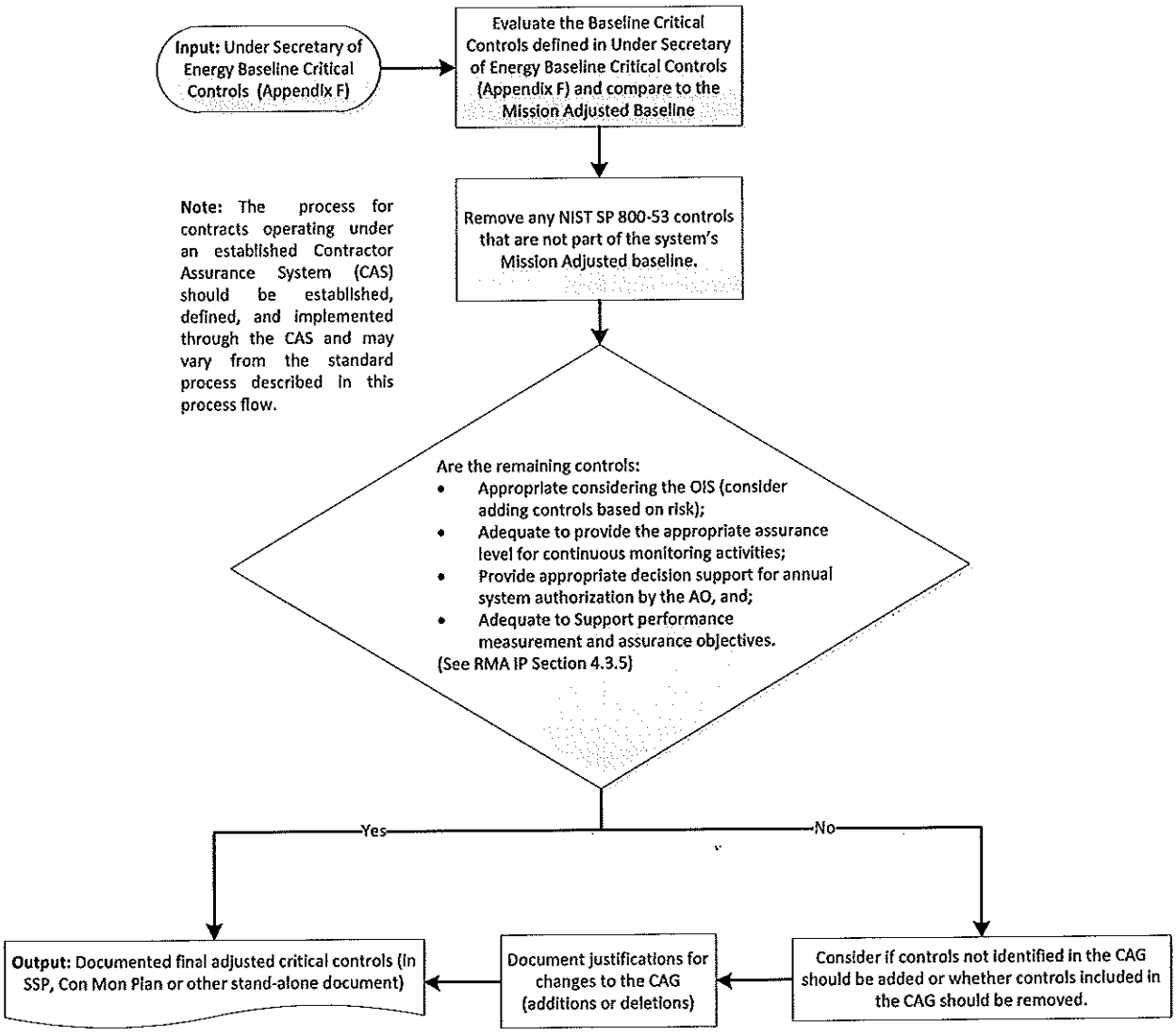


Exhibit 4: Under Secretary of Energy Control Evaluation Process

Appendix D: Summary of RMA Tasks

RMA TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
RMA Step 0: Assess Organizational Impact Levels		
TASK 0-1 **Business Dependencies** Gather artifacts related to the mission/business function, criticality of program systems and data, and known risk tolerance.	Risk Executive (Function)	Authorizing Official Information System Owner Information Owner/Steward
TASK 0-2 **Organizational Impact Analysis** Determine strategic impacts of loss to confidentiality, integrity, and availability of supporting information systems.	Risk Executive (Function)	Authorizing Official Information System Owner Information Owner/Steward
TASK 0-3 **Organizational Impact Statement** Prepare a statement of organizational impact based upon loss to confidentiality, integrity, and/or availability of supporting systems.	Risk Executive (Function)	Authorizing Official Information System Owner Information Owner/Steward
RMA Step 1: Categorize Information System		
TASK 1-1 **Security Categorization** Categorize the information system and document the results of the security categorization in the security plan.	Information System Owner Information System Security Manager Information Owner/Steward	Risk Executive (Function) Authorizing Official ***or*** Representative Under Secretary of Energy Cyber Security Program Manager Senior Information Security Officer Information System Security Officer
TASK 1-2 **Information System Description** Describe the information system (including system boundary) and document the description in the security plan.	Information System Owner Information System Security Manager	Authorizing Official ***or*** Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 1-3 **Information System Registration** Register the information system with appropriate organizational program/management offices. * FISMA systems only	Information System Owner	Senior Information Security Officer Information System Security Officer

RMA Step 2: Select Security Controls		
TASK 2-1 **Common Control Identification** Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).	Senior Information Security Officer Information System Security Manager	Risk Executive (Function) Authorizing Official ***or*** Representative Information System Owner
TASK 2-2 **Security Control Selection** Select the security controls for the information system and document the controls in the security plan.	Information System Security Manager Information System Owner	Authorizing Official ***or*** Representative Under Secretary of Energy Cyber Security Program Manager Information Owner/Steward Information System Security Officer
TASK 2-3 **Monitoring Strategy** Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation.	Information System Owner Information System Security Manager	Risk Executive (Function) Authorizing Official ***or*** Representative Under Secretary of Energy Cyber Security Program Manager Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 2-4 **Security Plan Approval** Review and approve the security plan.	Authorizing Official ***or*** Representative	Risk Executive (Function) Under Secretary of Energy Cyber Security Program Manager Senior Information Security Officer
RMA Step 3: Implement Security Controls		
TASK 3-1 **Security Control Implementation** Implement the security controls specified in the security plan.	Information System Owner	Information Owner/Steward Information System Security Manager Information System Security Officer
TASK 3-2 **Security Control Documentation** Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).	Information System Owner Information System Security Manager	Information Owner/Steward Information System Security Officer

RMA Step 4: Assess Security Controls		
TASK 4-1 **Assessment Preparation** Develop, review, and approve a plan to assess the security controls.	Security Control Assessor	Authorizing Official ***or*** Representative Under Secretary of Energy Cyber Security Program Manager Senior Information Security Officer Information System Owner Information Owner/Steward Information System Security Officer
TASK 4-2 **Security Control Assessment** Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.	Security Control Assessor	Information System Owner Information System Security Manager Information Owner/Steward Information System Security Officer
TASK 4-3 **Security Assessment Report** Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.	Security Control Assessor	Information System Owner Information System Security Manager Information System Security Officer
TASK 4-4 **Remediation Actions** Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.	Security Control Assessor	Authorizing Official ***or*** Representative Under Secretary of Energy Cyber Security Program Manager Senior Information Security Officer Information System Owner Information System Security Manager Information Owner/Steward Information System Security Officer
RMA Step 5: Authorize Information System		
TASK 5-1 **Plan of Action and Milestones** Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.	Information System Owner Information System Security Manager	Information Owner/Steward Information System Security Officer
TASK 5-2 **Security Authorization Package** Assemble the security authorization package and submit the package to the Authorizing Official for adjudication.	Information System Owner Information System Security Manager	Information System Security Officer Security Control Assessor
TASK 5-3 **Risk Determination** Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	Authorizing Official ***or*** Representative	Risk Executive (Function) Senior Information Security Officer

RMA Step 5 (continued): Authorize Information System		
TASK 5-4 **Risk Acceptance** Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.	Authorizing Official	Risk Executive (Function) Authorizing Official Representative Senior Information Security Officer
RMA Step 6: Monitor Security Controls		
TASK 6-1 **Information System and Environment Changes** Determine the security impact of proposed or actual changes to the information system and its environment of operation.	Information System Owner Information System Security Manager	Risk Executive (Function) Authorizing Official ***or*** Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 6-2 **Ongoing Security Control Assessments** Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.	Security Control Assessor	Authorizing Official ***or*** Representative Information System Owner Information System Security Manager Information Owner/Steward Information System Security Officer
TASK 6-3 **Ongoing Remediation Actions** Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.	Information System Owner	Authorizing Official ***or*** Representative Information Owner/Steward Information System Security Officer Security Control Assessor
TASK 6-4 **Key Updates** Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.	Information System Owner	Information System Security Manager Information Owner/Steward Information System Security Officer
TASK 6-5 **Security Status Reporting** Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the Authorizing Official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.	Information System Owner	Information System Security Manager Information System Security Officer

RMA Step 6 (continued): Monitor Security Controls		
TASK 6-6 **Ongoing Risk Determination and Acceptance** Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.	Authorizing Official	Risk Executive (Function) Authorizing Official Representative Senior Information Security Officer
TASK 6-7 **Information System Removal and Decommissioning** Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.	Information System Owner	Risk Executive (Function) Authorizing Official Representative Senior Information Security Officer Information System Security Manager Information Owner/Steward Information System Security Officer

Appendix E: Under Secretary of Energy Baseline Critical Controls

SANS Top 20 Critical Controls	Mapping to NIST SP 800-53 Revision 3 Controls
Critical Control 1: Inventory of Authorized and Unauthorized Devices	CM--8 (a, c, d, 2, 3, 4), PM--5, PM--6
Critical Control 2: Inventory of Authorized and Unauthorized Software	CM--1, CM--2 (2, 4, 5), CM--3, CM--5 (2, 7), CM--7 (1, 2), CM-- 8 (1, 2, 3, 4, 6), CM--9, PM--6, SA--6, SA--7
Critical Control 3: Secure Configurations for Hardware and Software	CM--1, CM--2 (1, 2), CM--3 (b, c, d, e, 2, 3), CM--5 (2), CM--6 (1, 2, 4), CM--7 (1), SA--1 (a), SA--4 (5), SI--7 (3), PM--6
Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	AC--4 (7, 10, 11, 16), CM--1, CM--2 (1), CM--3 (2), CM--5 (1, 2, 5), CM--6 (4), CM--7 (1, 3), IA--2 (1, 6), IA--5, IA--8, RA--5, SC--7 (2, 4, 5, 6, 8, 11, 13, 14, 18), SC--9
Critical Control 5: Boundary Defense	AC--17 (1), AC--20, CA--3, IA--2 (1, 2), IA--8, RA--5, SC--7 (1, 2, 3, 8, 10, 11, 14), SC--18, SI--4 (c, 1, 4, 5, 11), PM--7
Critical Control 6: Maintenance, Monitoring and Analysis of Security Audit Logs	AC--17 (1), AC--19, AU--2 (4), AU--3 (1,2), AU--4, AU--5, AU--6 (a, 1, 5), AU--8, AU--9 (1, 2), AU--12 (2), SI--4 (8)
Critical Control 7: Application Software Security	CM--7, RA--5 (a, 1), SA--3, SA--4 (3), SA--8, SI--3, SI--10
Critical Control 8: Controlled Use of Administrative Privileges	AC--6 (2, 5), AC--17 (3), AC--19, AU--2 (4)
Critical Control 9: Controlled Access Based on Need to Know	AC--1, AC--2 (b, c), AC--3 (4), AC--4, AC--6, MP--3, RA--2 (a)
Critical Control 10: Continuous Vulnerability Assessment and Remediation	RA--3 (a, b, c, d), RA--5 (a, b, 1, 2, 5, 6)
Critical Control 11: Account Monitoring and Control	AC--2 (e, f, g, h, j, 2, 3, 4, 5), AC--3
Critical Control 12: Malware Defenses	SC--18, SC--26, SI--3 (a, b, 1, 2, 5, 6)
Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services	CM--6 (a, b, d, 2, 3), CM--7 (1), SC--7 (4, 5, 11, 12)
Critical Control 14: Wireless Device Control	AC--17, AC--18 (1, 2, 3, 4), SC--9 (1), SC--24, SI--4 (14, 15)
Critical Control 15: Data Loss Prevention	AC--4, MP--2 (2), MP--4 (1), SC--7 (6, 10), SC--9, SC--13, SC--28 (1), SI--4 (4, 11), PM--7
Critical Control 16: Secure Network Engineering	IR--4 (2), SA--8, SC--7 (1, 13), SC--20, SC--21, SC--22, PM--7
Critical Control 17: Penetration Tests and Red Team Exercises	CA--2 (1, 2), CA--7 (1, 2), RA--3, RA--5 (4, 9), SA--12 (7)
Critical Control 18: Incident Response Capability	IR--1, IR--2 (1), IR--4, IR--5, IR--6 (a), IR--8
Critical Control 19: Data Recovery Capability	CP--9 (a, b, d, 1, 3), CP--10 (6)
Critical Control 20: Security Skills Assessment and Appropriate Training To Fill Gaps	AT--1, AT--2 (1), AT--3 (1)

Appendix F: References

Government Laws

Public Law 93-579, *Privacy Act of 1974*, December 31, 1974.

Public Law 104-106, Division E, *Clinger-Cohen Act of 1996 (formerly Information Technology Management Reform Act)*, February 10, 1996.

Public Law 107-347 [H.R. 2458], *The E-Government Act, Title II — Federal Management and Promote of Electronic Government Services,* and *Title III — Information Security Federal Information Security Management Act (FISMA)* December 17, 2002.

Government Paperwork Elimination Act, October 23, 1998.

Federal Acquisition Regulation (FAR)

Office of Management and Budget (OMB)

OMB Circular A-11, *Preparing, Submitting, and Executing the Budget*, updated annually.

OMB Circular A-123, *Management Accountability and Control*, June 21, 1995.

OMB Circular A-130, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources*, 2003.

OMB, *Government Performance and Results Act of 1993*, January 5, 1993.

Committee on National Security Systems (CNSS)

CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, October, 2009.

National Institute of Standards and Technology (NIST)

Federal Information Processing Standards (FIPS) Publications

FIPS Publication 140-1, *Security Requirements for Cryptographic Modules*, January 1994.

FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

FIPS Publication 201-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006.

Special Publications (SP)

Key NIST Series 800 SPs

NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010

NIST SP 800-39, Managing Information Security Risk, March 2011.

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

NIST SP 800-53A REVISION 1, *Guide for Assessing the Security Controls in Federal Information Systems*, June 2010.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

NIST SP 800-64 Revision 2, *Security Considerations in the SDLC,* October 2008

Department of Energy Resources

DOE M 470 4-1, *Safeguards and Security Program Planning and Management*, August 26, 2005.

DOE O 205.1B, *Department of Energy Cyber Security Program*, May 16, 2011.

DOE O 206.1, *DOE Privacy Program,* January 16, 2009.

DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, April 25, 2011.

DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, July 28, 2006.

DOE G 200.1-1 Appendix F, *Computer System Retirement Guidelines*