Department of Energy
Office of Science
Washington, DC 20585

Office of the Director

June 25, 2010

MEMORANDUM FOR WILLIAM TURNBULL
ACTING CHIEF INFORMATION OFFICER

FROM: W. F. BRINKMAN
DIRECTOR, OFFICE OF SCIENCE

SUBJECT: Office of Science (SC) Program Cyber Security Plan (PCSP)

Attached is SC's PCSP. This Plan has been developed in accordance with the Department of Energy (DOE) Order 205.1A, *DOE Cyber Security Management.* It was developed with Site Office and National Laboratory input which defined the cyber security direction for SC based on the Office of Chief Information Officer (OCIO) directives, National Policy, risk, and cost.

The PCSP establishes SC program cyber security requirements for both Federal and contractor staffs consistent with the OCIO's goals.

Attachment

cc w/attachment:
C. Woods, IM-31
G. Malosh, SC-3
M. Jones, SC-31
M. Sparks, SC-31.3
W. Dykas, SC-31.3

DEPARTMENT OF ENERGY

Office of Science

PROGRAM CYBER SECURITY PLAN

June 2010

This page intentionally left blank.

DEPARTMENT OF ENERGY
Office Science
PROGRAM CYBER SECURITY PLAN
June 2010

Executive Summary

The Office of Science (SC) Program Cyber Security Plan (PCSP) fulfills requirements of the Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*. The PCSP communicates the basic requirements that must be implemented to ensure effective cyber security protection for SC information and information systems. The standards and procedures are applicable to classified and unclassified information systems used at SC Federal entities and by contractors. This document will be updated biennially to reflect new cyber security risks and changes to national or departmental policy.

For Federal entities, this PCSP will be implemented through the SC Management System and is effective immediately. For contractors, the PCSP requirements are transmitted through Contractor Requirements Document of DOE O 205.1A.

Each organization will document its implementation of PCSP requirements in the site-level cyber security program plans and individual system security plans. The organization must develop and document a comprehensive plan that details a risk mitigation strategy for those components of the PCSP that will not be implemented. Weaknesses that are not addressed by the risk mitigation plans must be addressed with a Plan of Action and Milestones (POA&M). Each POA&M must be reviewed, approved, and monitored to completion by the cognizant Authorizing Official (AO).

Assurance and oversight of the SC Cyber Security Program is accomplished through SC line management directed assessments and evaluations of contractor assurance systems.

Approved: ____________ **Disapproved:** ____________ **Date:** JUN 25 2010

Dr. William Brinkman,
Director, DOE Office of Science

This page intentionally left blank.

TABLE OF CONTENTS

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
March 2, 2007	March 2, 2007	Update for NIST 800-53 R2, addition of National Security System Manual.	Entire Document	
20100610	6/10/2010	Major revision references NIST for process and requirements for unclassified systems. DOE manuals are not referenced. Replaces 2007 PCSP Exhibits for unclassified systems.	Entire Document	wd/yb

This page intentionally left blank.

1 Introduction

The United States Department of Energy (DOE) and the Office of Science (SC) is responsible for providing a sound cyber security management structure to ensure the protection of information and information systems. This responsibility is aligned to the overarching SC mission to advance the national, economic and energy security of the United States by promoting scientific and technological innovation. This mission relies on adequate and appropriate protection of information and information systems.

The Program Cyber Security Plan (PCSP) provides a foundation for ensuring the confidentiality, integrity, and availability of information and information systems at the SC locations. The PCSP uses the Risk Management Framework (RMF) described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1 (800-37R1), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

1.1 Purpose

The SC PCSP provides a mission-focused, risk-based process for cyber security management. The risk management strategy fosters the success of the varied missions of the SC Programs, and provides an agile and transparent process that is consistent with NIST guidance. The processes defined in this document are driven by the organization's business and mission requirements and are used to tailor cyber security requirements for SC information systems. The SC PCSP applies to all phases of the security life cycle and the system development life cycle.

1.2 Scope

All relevant security areas outlined by Federal law, NIST standards, and DOE directives are addressed in this document. All organizations within SC must utilize this PCSP for implementation and management of the site cyber security program. The PCSP requirements apply to all information systems and information collected, created, processed, transmitted, stored, or disseminated by or on behalf of the SC.

The PCSP roles, processes, and requirements use NIST documents as the primary resource for cyber security program planning, implementation, and management guidance. Where needed, SC or DOE implementation direction is provided for unique DOE or SC roles, processes, and specifications.

In the PCSP, the term site refers to the ten SC laboratories and associated site offices, the Chicago Office, the Oak Ridge Office, Oak Ridge Institute for Science and Education (ORISE), the Office of Science and Technical Information (OSTI), and the SC Headquarters. In the NIST documentation, the term organization is defined as a federal agency, or as appropriate, any of its operational elements.

1.3 The Office of Science Description

The SC is the single largest Federal government supporter of basic research in the physical sciences in the United States, providing more than 40 percent of the total Federal funding for this vital area of national importance. The program office oversees, and is the principal Federal funding agency of the Nation's research programs in high-energy physics, nuclear physics, fusion energy sciences, material sciences, and chemical sciences. The SC also supports vital U.S. research in climate change, geophysics, genomics, life sciences, and science education.

SC manages ten world-class laboratories, often called the "crown jewels" of our national research infrastructure. The program office administers the construction and operation of some of the most advanced research and development user facilities, including particle and nuclear physics accelerators, synchrotron light sources, neutron scattering facilities, supercomputers, and high-speed computer networks.

The SC research portfolio supports tens of thousands of principle investigators, post-doctoral students, and graduate students tackling some of the most challenging scientific questions of our era. The research process makes extensive use of peer review and Federal advisory committees to identify priorities and determine the scientific proposals with the greatest potential for scientific innovation. Research is conducted by groups that range in size from a single investigator to international collaborations that cross-institutional boundaries and utilize resources at universities and research centers around the world. The unique capabilities at the SC sites are used by other DOE organizations, commercial industry, and other government agencies. Landlord responsibilities at the SC sites include non-Science missions such as environmental management and may utilize the SC facilities and staff.

1.4 The Office of Science Risk Approach

The Office of Science risk approach uses the Risk Management Framework (RMF) described in the NIST SP 800-37R1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. The RMF requires use of Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems;* and NIST SP 800-53 Revision 3 (800-53R3), *Recommended Security Controls for Federal Information Systems and Organizations.*

SC organizations are required to use a graduated approach to risk management based on data sensitivity and the potentially negative impact associated with the loss of confidentiality, integrity, or availability of information or information systems. The graduated approach is implemented at the organizational level through the organizational risk management strategy and at the system level by utilizing appropriate baselines for FIPS 200 and NIST 800-53R3 security controls. Organizations will use the processes in this PCSP to determine and manage their security risk with appropriately adjusted processes and controls. The risk management approach provides appropriate information and asset protection and supports the site mission.

1.5 Interrelationship of PCSP and Security Plans

The PCSP documents the processes, responsibilities, and requirements for the SC cyber security program. The PCSP identifies cyber security requirements to be implemented in a site-specific cyber security program plan (CSPP) and the information system-specific system security plans (SSPs). Additional information on the PCSP, site CSPPs, and SSPs is in Section 3, Risk Management Framework and Control Selection.

Aspects of this PCSP that are not implemented are documented in a comprehensive plan that details a risk mitigation strategy for those components of the PCSP. Weaknesses not addressed by the risk mitigation plans will be addressed with a Plan of Action and Milestones (POA&M).

1.6 Change Management and Transition

The PCSP will be reviewed biennially and updated as needed to address new cyber security risks or changes to national or departmental policy. New Federal or DOE requirements will be incorporated into the PCSP after consultation with the SC Federal and contractor cyber security community. Changes will be communicated to SC sites and field elements through SC Management System (SCMS) for Federal staff and systems or through the contractor requirements document of DOE O 205.1A for service contractors or Management and Operating (M&O) contractors.

Information systems retain the current Authorization to Operate (ATO) until the end of the authorization period. Re-authorization is required when the system reaches the end of its three-year authorization period or there is a security-significant change. After the implementation of this PCSP, reauthorization of the information system will be in accordance with this PCSP.

Implementation and reaccreditation activities that are delayed because of infeasible or cost-prohibitive requirements will be documented in the POA&M within 90 days for Federal systems, or within the period required by site contracts for contractor systems.

This PCSP (June 2010) replaces or cancels the following sections of the March 2007 PCSP:

- Program Cyber Security Plan (March 2007);
- Designated Approving Authority (DAA) Overview (Exhibit 2);
- Continuous Monitoring Program for Unclassified Systems (Exhibit 3);
- Unclassified Information Systems (Exhibit 4); and
- Continuous Monitoring Program for National Security Systems (Exhibit 5).

Requirements for SC National Security Systems (NSS or classified systems) are contained in the following:

- Cyber Security Requirements for National Security Systems (Exhibit 6); and
- National Security System Program Cyber Security Plan (April 2007).

1.7 PCSP Point of Contact

The SC Senior Information Security Officer is the point of contact for the SC PCSP.

Name: Walter Dykas
U.S. Department of Energy
Office of Science
Office of Safety, Security and Infrastructure
Address: 19901 Germantown Road
Germantown, MD 20874
Telephone: 301-903-8226
Email: SC.PCSP@science.doe.gov

2 Roles and Responsibilities

Roles and Responsibilities applicable to this PCSP are described in NIST SP 800-37R1, Appendix D. Only unique DOE or SC roles for which there is no NIST equivalent are described below. DOE or SC roles that have names other than those used in NIST publications are cited as "formerly identified as."

Appendix E of NIST 800-37R1 summarizes the responsibilities for each role by task that comprises the Risk Management Framework (RMF). The SC implementation of RMF requirements are discussed in Section 3 of this PCSP.

2.1 Under Secretary for Science

The Under Secretary for Science (S-4) has an overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. The Under Secretary for Science is responsible for setting cyber security requirements for the Office of Science and its contractors as mandated by DOE O 205.1A.

2.2 Director of the Office of Science

The Director of the Office of Science (SC-1) has responsibility and authority for the work conducted at SC national laboratories. SC-1 serves as the DOE SC cognizant security authority for programs, operations, and facilities under the purview of SC to assure that effective programs are in place for the protection of SC interests from loss, damage, or other harm, whether intentional or unintentional. SC-1 has the responsibility for establishing policy and expectations as well as assuring performance. SC-1 is responsible for the management and implementation of Safeguards, Security and Emergency Management programs administered by SC.

2.3 Deputy Director of Field Operations

The Deputy Director of Field Operations (DDFO) (SC-3) is responsible for the performance of the Office of Science Cyber Security Program and is directly accountable to the Director for the Office of Science. The DDFO is responsible for the security of SC information and information systems used by Federal and contractor staff. SC-3 monitors the PCSP and performance issues, and ensures appropriate corrective actions are planned and implemented. SC-3 is the owner of the SCMS and thus recommends final policy to SC-1 on matters affecting safeguards and security performance within SC.

2.4 Associate Director for the Office of Safety, Security and Infrastructure

The Associate Director (AD) for Safety, Security and Infrastructure (SSI) is responsible for identifying changes in requirements, determining the impact of changes, determining how new requirements can be implemented at the SC facilities, updating the PCSP, and posting the updated PCSP to the SCMS and making it available to appropriate Contracting Officer

Representatives. The AD for SSI has overall responsibility for the strategic direction, advocacy, and budgeting for the SC Safeguards and Security and Cyber Security Programs.

2.5 Senior Information Security Officer

This role was formerly identified as the SC Program Office Cyber Security Program Manager (CSPM).

The SC Senior Information Security Officer (SISO) responsible for: (1) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements within SC; (2) assisting senior SC officials with their security responsibilities; and (3) in coordination with other officials, reporting on the overall effectiveness of the organization's information security program, including progress of remedial actions. The SC SISO serves as the primary information security liaison for SC to the organization's Authorizing Officials and Authorizing Official Designated Representatives, information system security managers (ISSM), and information system security officers (ISSO). The SC SISO ensures that cyber security requirements are implemented within the SC by monitoring cyber information and information system status reporting processes outlined in Section 3. Please see NIST SP 800-37R1, Appendix D.

2.6 Authorizing Official

The Authorizing Official (AO) was formerly identified as the Designated Approving Authority (DAA). Please see NIST SP 800-37R1, Appendix D. SC positions that are AOs are identified in Section 3, under Authorization to Operate.

2.7 Authorizing Official Designated Representative

This role was formerly identified as the Designated Approving Authority Representative. Please see NIST SP 800-37R1, Appendix D.

2.8 Risk Executive (Function)

In addition to the description in NIST SP 800-37R1, Appendix D, the Risk Executive function is performed at several organizational levels within DOE. The DOE Risk Executive function is performed by the Cyber Security Governance Council, consisting of the DOE Under Secretaries and the Chief Information Officer. The SC Risk Executive function is provided by the DDFO and site office managers. At the site level, Risk Executive function is performed through communication between the site office manager and site senior managers. For M&O or support contracts, the Risk Executive function is performed through communication between the site office manager and contractor senior management. Within each site, the site-level Risk Executive function directly supports implementation of the site cyber security program. Please see NIST SP 800-37R1, Appendix D.

2.9 Information System Security Manager

The ISSM has oversight responsibilities for the information security program at a single site or location. The ISSM is considered the lead cyber security person at the site and has knowledge of system functions, cyber security policies, and technical cyber security protection measures. The

ISSM performs the functions indicated for the Senior Information Security Officer indicated in the RMF, but at a site level. See Appendix D of NIST SP 800-37R1 for SISO responsibilities and footnote 58 for additional ISSM-related responsibilities.

2.10 Security Control Assessor

This role was formerly identified as Certification Agent. Please see NIST SP 800-37R1, Appendix D.

2.11 The Office of Science Integrated Support Center

The SC Integrated Support Center (ISC) provides services or functions for SC Field Elements at the request of the site office manager. These activities support the implementation of the SC PCSP requirements. Specific services provided are documented in the ISC service agreement.

3 Risk Management Framework and Control Selection

The RMF provides processes for: (1) evaluating the organizational impacts of cyber security actions; (2) categorizing information systems; (3) developing a mission-adjusted baseline of security controls; (4) deviating from selected security controls if necessary; (5) performing information system authorizations; and (6) implementing a continuous monitoring process.

The following paragraphs describe the DOE- and SC-specific implementation of NIST SP 800-53R3 Program Management (PM) controls, specify parameters for assignment and selection operations for site-implemented controls, and list common controls that sites will document if the site uses these as inherited controls. The SC parameter assignments are required and will be updated by the organization to reflect the local environment. Control parameters or selections of NIST SP 800-53R3, which are not specified below, will be specified in the site CSPP or in the individual SSPs.

In the descriptions below, where possible, the NIST SP 800-53R3 control (e.g., Control AU-1) or NIST SP 800-37R1 task (e.g., RMF Task 1-1) is indicated. The PCSP is the SC implementation of NIST SP 800-53R3 Program Management Controls. The PCSP is approved by the Director of the Office of Science.

3.1 The Office of Science Implementation and Parameter Assignments

Parameter assignments are provided for the identified controls from NIST SP 800-53R3.

1. PCSP Update: The PCSP is reviewed and updated every two years and when there is a security-significant change that potentially alters the risk accepted. Applicable to: RMF Task 1-1 and Control PM-1.

2. Program Management Controls: The PCSP implements Program Management controls at the SC-level. Sites will also implement Program Management controls at the site level. Applicable to: RMF Task 1-1 and Control PM-1.

3. Dash one controls: The site implementation of the PCSP is accomplished through the site-level CSPP and individual SSPs. The site will review and update the site policies which implement the NIST "dash one" controls (e.g., AU-1) at least annually. Applicable to: RMF Task 1-1 and Controls AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

4. National Security Systems: The source of the requirements, roles, and processes for SC National Security Systems (NSS or classified systems) are contained within the NSS portions of the SC Program Cyber Security Plan, *Cyber Security Requirements for National Security Systems* (March 2007) and *National Security System Program Cyber Security Plan* (April 2007). Applicable to: RMF Task 1-1 and Control PM-1.

5. Critical Infrastructure: The SC has no critical infrastructure related information systems. Applicable to: RMF Task 1-1 and Controls PM-8 and SA-14.

6. Information and Information System Categorization: Sites will categorize their information and information systems using FIPS 199 and the latest version of NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, or appropriate sponsor guidance for unique sponsor requirements, including DOE, non-DOE sponsors, or the local site. Applicable to: RMF Task 1-1 and Control RA-2.

7. Risk Management Framework: The NIST RMF is described as a sequential process in which some steps may be performed out of sequence or in parallel. The RMF is described as a system-level process, but it is also applicable to organizational levels or tiers. These levels are: (1) organizational or governance; (2) mission and business process; and (3) information system. The RMF step Categorize Information System provides a process for determining information system risk that includes an assessment of mission and business risk associated with the loss of confidentiality, integrity, or availability associated with the information system. This organizational risk assessment and impact is contributes to the overall site cyber risk assessment which may be included in the site CSPP, and included in the individual SSPs with resulting artifacts that include a business/ mission impact statement and, if appropriate, a contingency plan associated with the information system). Applicable to: RMF Task 1-1 and Control RA-2.

8. Security Plans: The PCSP documents the processes, responsibilities, and requirements for the SC cyber security program. The PCSP identifies cyber security requirements to be implemented in the site CSPP and information system specific SSPs. NIST SP 800-53R3 Control PM-1 indicates content required for the CSPP and Control PL-2 indicates the content required for CSPPs and SSPs. Applicable to: RMF Task 1-2 and Controls PL-1, PL-2, PM-1, CA-5, and CA-6.

   a. The site CSPP integrates individual SSPs and describes site common roles, requirements, controls, and processes. The CSPP is approved by the AO. The CSPP also defines how controls documented in the CSPP are tested as part of the authorization process. Common controls could also be documented, tested, and authorized in one or more separate SSPs. The CSPP does not need to be registered as a Federal Information Security Management Act (FISMA) information system. The site will also document and publish supporting site-level policies and procedures to support the site cyber security program implementation.
   b. The individual SSPs document the specifics of implementation for information systems. Common controls provided by the site or organizations external to the site for use by multiple site information systems will be documented in the CSPP or one or more SSPs.

9. Privacy and Private Information: Sites will use current contract or SCMS requirements to implement privacy or private information requirements and processes for reporting and protection of Privacy related information. Sites may have requirements imposed by state

or local jurisdictions. Applicable to: RMF Task 1-1 and Controls AC-21, IA-8, PL-1, PL-2, PL-5, PS-6 and RA-3.

10. Incident Point of Contact: Sites will provide point of contact information to the SC SISO and DOE Cyber Incident Response Capability (DOE-CIRC) for incident coordination that can be used for incident communication at any time of day. Incident communication and response will use the most current DOE cyber security incident requirements in contracts or SCMS. Applicable to: RMF Task 1-2 and Controls IR-1, IR-4, and IR-6.

11. Control Tailoring: Control tailoring will be performed at the organizational or system level. Tailoring decisions for all affected security controls including the rationale for those decisions, are documented in the information system security plan, and then approved by the AO as part of the security plan approval process. Applicable to: RMF Tasks 2-1, 2-2, and 2-3 and Controls PL-1, PL-2, and RA-3.

12. Plan of Action and Milestones: POA&M items are weaknesses, deficiencies, or vulnerabilities identified by assessments internal or external to the organization or information system being assessed or as part of the continuous monitoring strategy. Weaknesses are reviewed by the organization and the AO. Weaknesses that indicate an unacceptable residual risk and impact to the ATO of the information system will be recorded as a system-level or program-level POA&M with corrective measures identified. The POA&M list is part of the information system authorization package. The POA&M will be documented, updated, reported, and tracked as FISMA POA&M by the organization and the AO. Applicable to: RMF Task 5-2 and Controls PM-4, CA-5, and CA-6.

13. Security Authorization Package: The security authorization package contains the information system security plan (e.g., risk statement, risk and assessment strategy), the security assessment (includes certification activities and weaknesses), and the POA&M. A site-level security authorization package should provide a basis for cyber security input into a contractor assurance system when combined and coordinated with other contractor assurance activities. Applicable to: RMF Task 5-2 and Controls PM-4, CA-5, and CA-6.

14. Authorization to Operate: The ATO is granted by the SC AO who is: (1) the site office manager for each site or site office; (2) the office manager (for SC-Chicago, SC-Oak Ridge); the OSTI senior manager; or (3) the Contracting Officer for ORISE. The SC SISO maintains the list of SC AOs. Applicable to: RMF Task 5-3 and Controls PM-10 and CA-6.

15. Reauthorization: Security authorization periods for SC information systems are three years based on continuing acceptable residual risk that is accepted by the AO. Reauthorization is required for a security-significant change causing unacceptable residual risk. The authorization period can be extended by the AO on an annual or ongoing basis for information systems with acceptable residual risk; an effective continuous monitoring process to assess and manage threats, vulnerabilities, and risk; and

processes to inform the AO of the security state of the information system. Applicable to: RMF Task 5-3, RMF Step 6, and Controls CA-1 and CA-6.

16. Significant Change or Security-Significant Change: Unless addressed through ongoing authorization activities and continuous monitoring, security-significant changes have the potential to alter the residual risk accepted by the AO, defined by the authorization package and can trigger the immediate need to assess the security state of the information system and modification of the authorization package. Organizations will define security-significant changes for the information system and local environment. Security-significant changes include the following:

    a. An incident that results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;
    b. A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation. These are identified based on intelligence information, law enforcement information, or other credible sources of information;
    c. Changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware, or changes in the operational environment which affect the security state of the system; or
    d. Changes to the organization, organizational risk management strategy, information security policy, supported missions and/or business functions, or information being processed, stored, or transmitted by the information system.

    Applicable to: RMF Task 6-1 and Control CA-6.

3.2 The Office of Science Common Control Implementation

Common controls identified below are Departmental, enterprise, or site-wide processes that implement certain NIST SP 800-53R3 controls. The common control provider is responsible for providing appropriate authorization documentation. Sites will document the local implementations of these controls if the site relies on the common control to mitigate risk. The following are DOE-wide processes that sites may implement locally.

1. Cyber Information and Information System Status Reporting: The SC uses the DOE Office of the Chief Information Officer (OCIO) processes for quarterly and annual status reporting of:

    a. FISMA information security performance metrics (Control PM-6)
    b. Plan of Action and Milestones (POA&M) (Controls PM-4, CA-5)
    c. Capital Planning and Improvement Control (Control PM-3)
    d. Enterprise Architecture (Control PM-7)
    e. Information System Inventory (Control PM-5).

Sites will use the quarterly schedule to review and update the site-specific information. The SC will coordinate data call communications with the site office or office manager. Applicable to: RMF Task 2-1 and RMF Task 6-5.

2. Privacy Data Reporting: The DOE Office of Privacy provides a process for quarterly and annual reporting of privacy related information. Sites will use the quarterly schedule to review and update the site-specific information. SC will coordinate data call communications with the site office or office manager. Applicable to: RMF Tasks 2-1, and 6-5 and Controls AC-21, IA-8, PL-1, PL-2, PL-5, and PS-6.

3. Public Key Infrastructure: The DOE OCIO provides a DOE enterprise Public Key Infrastructure (PKI) capability. Sites will document a local PKI implementation if one exists. Applicable to: RMF Task 2-1 and Control IA-5.

4. Incident Response: All cyber security incidents, including privacy breaches, must be identified, mitigated, categorized, and reported to the DOE-CIRC in accordance with DOE-CIRC procedures and guidance. Applicable to: RMF Task 2-1 and Control IR-1.

5. Intrusion Detection: DOE provides enterprise intrusion detection capabilities, including the Cooperative Protection Program and the Cyber Federated Model. Sites will document the local implementation of these capabilities, if used. If not used, the site will document the local implementation of site-level intrusion detection and prevention controls if the site relies on the common control to mitigate risk. Applicable to: RMF Task 2-1 and Control SI-4.

6. Assurance and Oversight: SC assurance and oversight are accomplished through line management directed assessments, confirmation of contractor assurance systems and internal and external reviews. The DOE-SC assurance approach relies on a close partnership between the local site office, the contractor, and the contractor's corporate parent. In this partnership, the contractor and corporate parent provide assurance to DOE that is transparent and allows DOE to leverage the contractor's processes and outcomes and confirm their effectiveness. Internal assessments are self-directed by the organization of the information system being assessed and include continuous monitoring of the information system.

    a. Independent assessments can be external or directed by the organization. Cyber security assessments may be performed by the SC ISC at the request of the site office manager. The ISC assessments can be used as an independent evaluation of the cyber security program.

    b. Weaknesses that indicate an unacceptable residual risk and impact to the information system ATO will be recorded as site system or program POA&M with corrective measures identified. The POA&M list is part of the information system authorization package. SC also enters deficiencies identified by the OIG into the Departmental Audit Report Tracking System (DARTS). DARTS is also used to track completion of associated corrective actions. Findings from security surveys and any classified findings are also entered into the Safeguards and Security Information Management System.

Applicable to: RMF Task 6-4 and Controls CA-2, CA-5, CA-6, CA-7, SA-9, and PM-3.

Appendix

Appendix A: Acronym List

AD	Associate Director
ATO	Authorization To Operate
AO	Authorizing Official (formerly DAA)
CSPM	Cyber Security Program Manager (now SISO)
CSPP	(site) Cyber Security Program Plan
DAA	Designated Approving Authority (now AO)
DDFO	Deputy Director of Field Operations
DOE	Department of Energy
DOE-CIRC	DOE Computer Incident Response Capability
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ISC	Integrated Support Center
ISSM	Information System Security Manager
ISSO	Information System Security Officer
M&O	Management and Operating (contract)
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ORISE	Oak Ridge Institute for Science and Education
OSTI	Office of Scientific and Technical Information
PCSP	Program Cyber Security Program (Plan)
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SC	Office of Science
SC-1	Director, Office of Science
SC-3	Office of Science, Deputy Director of Field Operations
SCMS	SC Management System
SISO	Senior Information Security Officer (formerly CSPM)
SP	Special Publication
SSP	System Security Plan