Cyber Security Technical and Management Requirements

Certification and Accreditation (TMR-2)
October 10, 2007

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs). This TMR document provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

Federal Agencies are required by Office of Management and Budget (OMB) Circular A-130, Appendix III, to establish a process to ensure that adequate security controls are provided for all information systems. The proper implementation of a certification and accreditation (C&A) process ensures that all applicable requirements have been integrated into the development and operational processes. The C&A process implements the concept of "adequate security," or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. The Department expects that all systems complete the C&A process prior to going operational (i.e., processing live data or information).

This TMR establishes a risk-based approach to C&A that is to be covered in each PCSP. It also provides guidance for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems,* and NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*. Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

Cancellations

This TMR replaces DOE CIO Guide 205.1-2, *Certification and Accreditation Guide,* dated March 2006.

Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

Requirements

TMR-2-1, Senior DOE Management Basic C&A Requirements

Senior DOE Management is responsible for developing, documenting, and implementing a certification and accreditation management program for all operating units, programs, and systems. The Senior DOE Management C&A program is to be documented in the PCSP and include the following requirements.

1. Each General Support System (GSS) or Major Application (MA) must be accredited or have Interim Approval to Operate (IATO) from the Designated Approving Authority (DAA) before any DOE/Government information is processed, created, transmitted, etc. on the system.
2. Each information system must be re-accredited at least every three years or whenever a security-significant change is to be made to the information system or its environment (physical, logical, or operational). Existing accreditations should remain valid until the system has passed the 3-year accreditation expiration date or security-significant changes have occurred.
3. The C&A activities must be based on the C&A Package as described in TMR-2-3.
4. Each information system shall be accredited using one of the following forms of accreditation.
    a. System accreditation for a single information system operating under a single System Security Plan (SSP). Accreditation is based on information system certification.
    b. Site accreditation to accredit multiple instances of an information system where all identical installations (instantiations) of the information system are located at an operating unit facility(ies). Each instantiation of the information system is implemented using the same SSP. Accreditation is based on the certification of the first system and the approval of processes for testing and certifying additional instantiations. The authority to operate additional instantiations under the SSP is based on successful completion of the follow-on processes described in the SSP.
    c. Type accreditation to accredit multiple instances of an information system where instantiations of the information system are located at different operating unit facility(ies) but a single DAA is responsible for the system. Each instantiation of the information system has been implemented using the same SSP. Accreditation is based on the certification of the first system and approval of processes for testing and certifying additional instantiations. The

authority to operate additional instantiations under the SSP is based on successful completion of the follow-on processes described in the SSP.

5. Training requirements for all personnel involved in C&A activities are to be documented.
6. The DAA may withdraw accreditation based on determination that the risk to the information is no longer acceptable.

TMR-2-2, PCSP C&A Process

The Senior DOE Management PCSP must document an organizational C&A process to be used by all operating units, programs, and systems. The C&A process is to establish a common approach for the specific tasks and sub-tasks necessary to complete the assessment and approval of an information system. The Senior DOE Management C&A process must include the following phases, and the PCSP must also specify the required formats for documentation in each phase as noted below.

1. C&A Initiation Phase. The System Owner identifies the information system composition, categorizes the system, reviews the DOE Enterprise Architecture for application to the system, determines the applicable security controls, examines the security environment (physical, logical, and operational) for any additional control requirements, identifies resources, develops the SSP, develops the contingency plan, and obtains approval of the SSP from the DAA. The Initiation phase allows an organization to quickly determine the information system security status and what changes have to be made to attain or maintain compliance with the Senior DOE Management PCSP and other higher level Federal requirements. The initiation phase is composed of three tasks.
   a. Preparation. The preparation task develops the SSP and confirms that the contents of the plan are consistent with an initial assessment of risk. The Senior DOE Management PCSP must specify any required process, methodology, and format for the privacy impact assessment, risk assessments, system support and interconnectivity agreements, the Configuration Management Plan, and the Contingency Plan. The preparation task is composed of six sub-tasks.
      (1) Information System Description – The System Owner confirms that the information system has been fully described and documented in the SSP.
      (2) Security Categorization – The System Owner confirms that the information system has been categorized according to the applicable PCSP, the categorization has been documented in the SSP, and any needed contingency planning has been initiated.
      (3) Threat Identification – The System Owner confirms that potential threats have been identified and documented, including any resulting from existing or planned interconnection with other systems.

(4) Vulnerability Identification – The System Owner confirms that vulnerabilities to the system have been identified and documented in the Risk Assessment.

(5) Initial Risk Determination – The System Owner confirms that all risks have been identified and documented in the Risk Assessment and Privacy Impact Assessment.

(6) Security Control Identification – The System Owner confirms that implemented and planned security controls are documented in the SSP.

b. Notification and Resource Identification. The Notification and Resource Identification task informs Senior DOE Management that a C&A is underway. Resources are identified, and a system Plan of Actions and Milestones (POA&M) is prepared for C&A activities, if appropriate. The Notification and Resource Identification task is composed of two sub-tasks.

(1) Planning and Resources – The System Owner coordinates with the stakeholders to determine the level of effort and corresponding resources needed to accomplish C&A. A POA&M is then created for execution and budget input.

(2) Notification – The System Owner notifies all stakeholders that C&A activities are to be accomplished and provides the POA&M to the DAA.

c. SSP Analysis and Acceptance. The SSP Analysis and Acceptance task requires an independent review of the security categorization, an analysis of the SSP, evaluation of the Risk Assessment, and a formal acceptance of the SSP by the DAA. This task is composed of four sub-tasks.

(1) Security Categorization Review- An independent review of the security categorization documented in the SSP is accomplished by the DAA and Certification Agent.

(2) System Security Plan Analysis - An independent review of the SSP is completed by the DAA and Certification Agent to determine if the documented vulnerabilities, threats, and associated risks are accurate and the implemented and planned controls are sufficient.

(3) System Security Plan Update – The System Owner updates the SSP with any findings from the independent reviews.

(4) System Security Plan Acceptance – The DAA reviews the SSP to determine if the documented risks are acceptable and provides written approval of the SSP for C&A activities prior to progressing to the next phase.

2. Certification Phase. The Certification phase demonstrates, through independent validation using specified verification techniques and procedures, the security controls for the information system have been implemented correctly and are

effective in their application. The Certification Agent selects or develops Security Test and Evaluation (ST&E) procedures to perform an assessment of each security control; all selected procedures must be approved by the DAA. Using the approved procedures, the Certification Agent assesses each control and prepares the ST&E Report and the Security Assessment Report (SAR). The System Owner assembles the Certification Package. The certification phase consists of three tasks.

a. Security Control Assessment. This task produces test and evaluation procedures and conducts and documents an accurate assessment of the security controls. This task is composed of two sub-tasks:

   (1) Documentation and Supporting Materials – The System Owner and the Certification Agent compile all relevant documentation and materials from the previous phases needed for security control assessment.

   (2) Methods and Procedures – ST&E procedures must be approved by the DAA prior to the conduct of control assessment. The ST&E procedures to be used for future instantiations for Site and Type forms of accreditation must be included as part of the ST&E procedures. The instantiation procedures must include the following:

      (a) The controls and ST&E procedures to be used by the Certification Agent to assess those controls in all future instantiations.

      (b) Provisions to identify the Certification Agent assessing each instantiation.

b. Security Assessment. The Certification Agent performs an evaluation of the security controls in place using the ST&E procedures to assess whether the controls identified in the SSP are implemented and operating as intended. The results of the evaluation are recorded and the ST&E Report finalized. For moderate and high impact systems, as categorized by DOE CIO TMR-1, and for all Protection Indices, as categorized by DOE M 205.1-4, the System Owner cannot act as the Certification Agent. The Certification Agent or designee must be independent of the system development and operations teams. NOTE: For a low impact unclassified system, a self-assessment can be substituted for ST&E. If a control fails the ST&E process, the control implementation can be corrected and re-assessed.

c. Certification Documentation. This task provides the certification findings to the System Owner, updates the C&A package as needed, prepare/update the POA&M(s), and assembles the accreditation package. This task is composed of five sub-tasks.

   (1) Findings and Recommendations – The Certification Agent makes recommendations for correcting any deficiencies or reducing and/or eliminating vulnerabilities in the SAR. The Certification Agent provides the System Owner with the SAR.

(2) C&A Package Update – The System Owner updates the SSP and Risk Assessment based on the SAR and any modifications or deviations to the security controls.

(3) Plan of Actions and Milestones – The System Owner updates the POA&M and creates any additional POA&M(s) to identify the milestones and schedule for addressing any issues and recommendations identified in the SAR. It is expected that all issues will be resolved by control implementation updates or through a deviation process (see TMR-2-3, paragraph 2) prior to Certification Package transmittal to the DAA.

(4) Deviations Risk Assessment – The System Owner must complete an updated Risk Assessment for any deviations proposed or approved.

(5) Certification Package Assembly – The System Owner assembles the final certification package and submits it to the DAA.

3. Accreditation Phase. The purpose of the accreditation phase is to determine if remaining vulnerabilities pose an acceptable level of risk. The decision can be an authorization to operate (accreditation), an Interim Authorization to Operate (IATO), or a denial of authorization to operate. The DAA decides, based on the evidence provided in the Certification Package and any independent evaluations requested or completed by the DAA, if the information system can operate at an acceptable level of risk. An Accreditation Letter is issued based on that decision. The DAA decision can take three forms.

- Accreditation. The information system is authorized to operate as specified in the Certification Package.
- Interim Authority to Operate (IATO). An IATO means that the information system is authorized to operate but has deficiencies that must be corrected. The deficiencies must not present any adverse impacts on the confidentiality of the information on the system. The DAA, Certification Agent, and System Owner must agree on the proposed correction and time frames. The System Owner must prepare a POA&M for each proposed correction. The Accreditation Letter must identify the end of the IATO period not to exceed 6 months.
- Denial. The DAA decides that the residual risk is too great and denies authorization to operate.

The accreditation phase consists of two tasks.

a. Accreditation Decision. The purpose of this task is to evaluate the impact of risks and determine whether the level of risk is acceptable. This task is composed of two sub-tasks.

(1) Final Risk Determination – The DAA determines the overall risk based on the evidence presented in the final certification package and any independent evaluations requested or conducted by the DAA.

(2) Risk Acceptability – The DAA determines whether or not the residual risk is at an acceptable level. A final accreditation decision letter is then prepared.

b. Accreditation Documentation. The purpose of this task is to create and disseminate the final accreditation package. This task is composed of two sub-tasks.

(1) Accreditation Package Transmission – The DAA provides copies of the final Certification Package with original accreditation decision letter to the System Owner.

(2) System Security Plan Update – The System Owner updates the Certification Package to form the C&A Package with the results of the accreditation process.

4. Continuous Monitoring Phase. The Continuous Monitoring phase provides oversight and monitoring of security controls by the System Owner on an ongoing basis. This activity includes monitoring a select set of controls on a continuous basis and establishing processes that identify when security-significant changes have been made to the information system (configuration management) or the environment (physical, logical, or operational) that would warrant re-accreditation. This phase consists of three tasks.

a. Configuration Management and Control. The purpose of this task is to define and document a baseline system configuration and document and assess proposed and actual changes to the information system. This task is composed of two sub-tasks.

(1) Documentation of the Information System Changes – The System Owner documents the proposed and actual changes to the system and compares these to the baseline configuration.

(2) Security Impact Analysis – The System Owner analyzes proposed and actual changes to the system to determine the security impact.

b. Security Control Monitoring. The purpose of this task is to detect unauthorized changes to the system configuration through continuous monitoring and periodic assessment of a selected set of controls. This task is composed of two sub-tasks.

(1) Security Control Selection – The System Owner selects the technical, operational, assurance, and management security controls for continuous monitoring and periodic assessment.

(2) Selected Security Control Assessment – The System Owner assesses the controls designated to be monitored continuously and performs self-assessments periodically on the remaining controls.

c. Status Report and Documentation. The purpose of this task is to update the C&A Package, update the POA&M, and report the security status of the information system to the DAA. This task is composed of three sub-tasks.

(1) System Security Plan Update – The System Owner updates the C&A Package based on the changes identified from the Continuous Monitoring activities and begins the Initiation Phase for reaccreditation due to security-significant change(s).

(2) Plan of Action and Milestones Update – The System Owner updates the POA&M and creates any additional POA&M(s) to identify the milestones and schedule for addressing any issues and recommendations identified through Continuous Monitoring activities.

(3) Status Reporting – The System Owner reports the security status of the information system to the DAA.

TMR-2-3, Elements of C&A Package

The Senior DOE Management PCSP is to specify the required documentation and related formats for each phase of the organizational C&A process to be used by all operating units, programs, and systems. At a minimum, the documentation generated by the C&A process must include the following.

1. Approved System Security Plan –A SSP must be developed and implemented for all information systems. The SSP provides the system impact level, types of information processed, security requirements for the system, and a description of the security controls in place or planned for meeting those requirements. The SSP provides information necessary to secure an information system throughout its life cycle. However, the SSP need not contain all security documentation; it may be part of a hierarchy of security documents. Designated officials within the Senior DOE Management organization review and approve the SSP. Final approval is provided by the DAA. The SSP consists of two major parts: the System Description and the System Component Implementation.

   a. The System Description. The System Description defines the information system composition in terms of one or more system components that will implement the security controls, the information resident on the system, an overview of the security environment (physical, technical and operational) in which the system will reside, and the identification of any additional controls resulting from the evaluation of the security environment or required by the System Owner. The System description must address the following information:

   (1) Management Information: Provide an overview of the system purpose (e.g., machine controller, office desktop, etc), the organization, and the personnel responsible for system security (DAA, System Owner, Certification Agent, Information System Security Officer [ISSO], etc.).

(2) System Categorization: Identify all information types that are intended to be on the system and categorize the information system based on the security objectives (confidentiality, integrity, and availability). DOE CIO TMR-1 and DOE Manual 205.1-4 provide information on system categorization.

(3) System Composition: Identify the system components, the accreditation boundary, the form of accreditation, and provide an overview of the hardware and software that make up the information system.

(4) Physical Security Environment: Describe the physical environment (type of protection areas [e.g., Property Protection Area, Limited Area, Vault Type Room, etc.], physical and visual access controls, etc.) in which all system components must reside. Identify any physical threats that cannot be mitigated by the minimum security criteria.

(5) Logical Security Environment: Describe the function of each system component (user workstation, application server, router, switch, etc) and the system component interfaces and connections to networks outside the system boundary (e.g., a drawing showing network connectivity, etc.). Identify other systems with which the system component communicates and the connection rules and any threats that cannot be mitigated by the minimum security criteria.

(6) Operational Environment: Identify the user's required access authorization and processes for Need-to-Know control. For Site and Type forms of accreditation, identify the management processes and roles for acceptance of future instantiations of system components. Identify any operational threats that cannot be mitigated by the minimum security criteria.

(7) System Security Requirements: Identify the system categorization that will be assigned to all system components and used to determine the minimum security criteria. Identify any additional controls introduced to mitigate new threats or required by the System Owner. Identify any deviations from the security controls identified.

b. System Component Implementation. A system component implementation description must be developed for each system component and incorporated into the SSP. The system component implementation includes:

(1) System Component Overview: Describe the hardware/ software that provide the system security controls implementation for the system component, including networking interfaces.

(2) System Component Controls: Describe how each technical, operational, management, and assurance control is implemented. If all or part of a control is to be implemented by another system or system component (i.e., network logon, central backup, common security

controls, etc.), identify the system or system component that implements the control.

c. Interconnection Agreements. The Interconnection Agreement describes the management and technical operation between information systems (see DOE CIO TMR-5, *Interconnected Systems Management*).

(1) Memorandum of Understanding (MOU) –The MOU describes the management agreement between System Owners of interconnected information systems. The MOU specifies the security management responsibilities of each System Owner for the secure operation of the interconnection and authorizes the interconnection.

(2) Interconnection Security Agreements (ISA) - The ISA specifies the technical security implementation of the interconnections of two systems.

2. Security Risk Assessment. The completed risk assessment demonstrates the reduction in risk by applying security controls and identifies the residual risk involved with operating the information system. The Risk Assessment (RA) family of security controls in DOE CIO TMR-1 and DOE M 205.1-4 provide further information in this area. The following risk assessments supporting the SSP are to be attached as needed:

a. Risk assessment – The mitigation of the new threats or vulnerabilities identified during the physical, logical, or operational reviews must be supported with a risk assessment that justifies their mitigation.

b. Deviation risk assessment – Deviations must be supported with a risk assessment that identifies the risks to be accepted, compensatory measures, or alternative controls to be implemented.

3. Completed Privacy Impact Assessments - Privacy impact assessments provide an analysis of how Personally Identifiable Information (PII) is handled; evaluate security control compliance with legal, regulatory, and policy requirements; determine risk to the information; and evaluate the controls used to mitigate the risks.

4. Configuration Management Plan – The Configuration Management Plan defines the methodology for configuration change control during system development, tracking security flaws, authorization of changes, and, for the Certification and Accreditation process, provides documentation of the methodology and its implementation. The Configuration Management Plan may be included in the package or referenced.

5. Contingency Plan – Contingency planning determines the necessary procedures required to protect the continuing performance of core business functions and services, including information services, during an outage. The Contingency Plan may be included in the package or referenced.

6. Security Test & Evaluation Report – A comprehensive report resulting from the ST&E of all security controls for the information system and any later instantiations implemented under the Site or Type forms of accreditation. The results are used to

determine whether the controls in the approved SSP are implemented and operating as intended and are effective in a particular environment and to identify vulnerabilities in the system after the implementation of controls.

7. Plan of Action and Milestones - The POA&M documents the C&A activities for system development and system security configuration changes resulting from functional modifications, correction of deficiencies noted during assessments, or reduction or elimination of vulnerabilities.
8. Security Assessment Report[1] - A SAR is prepared and signed by the Certification Agent and references other completed certification documentation. The report provides (i) the results of assessing the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements; (ii) recommended POA&M, if there are deficiencies or known vulnerabilities remaining, and (iii) recommendation to the DAA regarding accreditation.
9. Accreditation Decision Letter - The accreditation decision letter transmits the DAA accreditation decision. The DAA attaches the certification documentation to the original accreditation letter and transmits it to the System Owner.

TMR-2-4, Operating Unit C&A Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement C&A policies and procedures compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization's environment and specific needs.

[1] Typically referred to as a Certification Letter.