Cyber Security Technical and Management Requirements

Security Testing and Evaluation (TMR-21)
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).

Security Testing and Evaluation (ST&E) is an essential element of the certification and accreditation (C&A) process. Throughout the system life cycle, ST&E is used to determine the system's compliance with defined security requirements and document the effectiveness of security control implementations. This TMR provides Senior DOE Management direction and minimum requirements for unclassified and National Security Systems to be incorporated in each PCSPs to assure the functionality, operation, and strength of security controls that have been documented in the system security plan (SSP) and implemented in an information system. The National Institute for Science and Technology (NIST) Special Publication (SP) 800-53A (DRAFT), *Guide for Assessing the Security Controls in Federal Information Systems*, may be used as a supplement for developing the Senior DOE Management PCSP and any related operating unit documentation required by the PCSP. NIST SP 800-42, *Guideline on Network Security Testing*, is also covered by the requirements of this document. 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 Guidance CS-37, *Security Testing Guidance*, dated January 2007.

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-21-1, Senior DOE Management ST&E Policy and Processes

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing ST&E policy and processes for all operating units, programs, and systems. The Senior DOE Management PCSP is to describe ST&E processes to include the following requirements.

1. The personnel responsible for approval, implementation, and management of ST&E processes are to be identified.

2. All controls identified in each SSP are to be subjected to security control assessment procedure(s) during the C&A process (see DOE CIO TMR-2, *Certification and Accreditation)* to evaluate the status of control implementation with respect to security requirements and effectiveness.

   a. Under a "System" form of accreditation, each control must be subjected to an ST&E process.

   b. Under a "Site or Type" form of accreditation, each control of the first installation (i.e., instantiation) of a system must be subjected to an ST&E process.

      (1) Accreditation of additional instantiation (identical installation) may be based on a subset of the ST&E procedures used for the first instantiation. This subset, which is identified in the ST&E Procedures and approved by the Designated Approving Authority (DAA), must provide for overall assurance that future instantiations are implemented identically to the first instantiation.

      (2) The ST&E procedure(s) used for the assessment/evaluation of a control for each additional instantiation must not be modified from those used to evaluate the original instantiation.

3. ST&E procedures must be approved by the DAA prior to the beginning of the ST&E process. The DAA may specify additional ST&E processes as part of C&A activities.

4. If Common Security Controls are used, processes are in place to assess, conduct ST&E, and assure the controls are implemented in an accredited system.

   a. ST&E for the reuse of Common Security Controls is not needed for each system if the implementing system remains accredited.

   b. Common Security Control ST&E results for subsequent systems are to reference the system accreditation date and SSP under which the control was first evaluated.

TMR-21-2, ST&E Documentation

The Senior DOE Management PCSP is to specify required ST&E documentation to be prepared and maintained by all operating units, programs, and systems. At a minimum, the documentation must include the following.

1. ST&E Procedures
   a. The ST&E procedures must associate each control described in the SSP with specific procedure(s) used to assess the control. Each ST&E procedure, at a minimum, verifies the security control(s) is in effect and correctly implements the explicitly identified functional criteria in the control statement. ST&E procedure(s) must be developed for each control identified in the SSP. The following assessment methods can be used.
      (1) Interview: Focused discussions with individuals or groups to facilitate understanding, achieve clarification, or obtain evidence.
      (2) Examine: Checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
      (3) Test: Exercising one or more assessment objects under specific conditions to compare actual with expected behavior.
   b. Each ST&E procedure must identify the specific control and associated assessment method(s) used to evaluate the control and support the determination of security control effectiveness. For unclassified systems, the assessment method attributes of depth, coverage, and type must be reflected in each ST&E procedure as described in Attachment 1. For National Security Systems (NSS), the assessment method attributes are described in the following paragraph.
   c. The NSS ST&E procedures must address the following attributes in the assessment procedures.
      (1) For NSS where the Confidentiality Consequence of Loss (CoL) is Medium, the ST&E process focus is on the control being in place, performing the functional requirements detailed in the SSP, and being operational with no obvious errors.
      (2) For NSS where the Confidentiality CoL is High, the ST&E process focus is on the control being in place, performing the functional requirements detailed in the SSP, being operational and correctly implemented, flaws uncovered are addressed, and the control incorporates the specific capabilities identified in the control statement.
      (3) For NSS where the Confidentiality CoL is Very High, the ST&E process focus is on the control being in place, performing the functional

requirements detailed in the SSP, being operational and correctly implemented, flaws uncovered are addressed, and the controls incorporate the specific capabilities identified in the control statement. The ST&E process focus is expanded to include verifying that the underlying internal function(s) of the control cannot be used to defeat or bypass the control and the design, implementation, and integration of the control are documented and the control is tested for the specific capabilities identified in the control statement as well as the underlying internal control functions.

d. Expected Results for Unclassified Systems. The expected results of ST&E procedures must assure that all management, operational, and technical controls are specified, implemented, and operational consistent with the functional requirements of the control statement. The following describes the level of detail necessary, by system Security Category, for the expected results.

(1) Low impact.

(a) The security control is in effect and meets explicitly identified functional requirements in the control statement.

(b) The control is in place, no obvious errors exist, and as flaws are discovered they are addressed in a timely manner.

(2) Moderate impact.

(a) The security control is in effect and meets explicitly identified functional requirements in the control statement.

(b) The System Security Plan (SSP) describes the functional properties of the control with sufficient detail to permit analysis and testing and includes assigned responsibilities and specific actions to ensure that the implemented control will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

(c) To ensure correct implementation and operation, each control incorporates specific capabilities and/or produces specific documentation.

(d) There are no obvious errors in the security control and it is implemented correctly and operating as intended.

(3) High impact.

(a) The security control is in effect and meets explicitly identified functional requirements in the control statement.

(b) The SSP provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control (including functional interfaces among control components). The SSP also includes assigned responsibilities and specific actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

(c) The developer/implementer is expected to provide the design, development, implementation, and component/ integration testing of the controls and to produce associated design and implementation documentation to support these activities.

(d) There are no obvious errors in the control, the control is implemented correctly and operating as intended on an ongoing and consistent basis, and there is continuous improvement in security control effectiveness.

e. Expected Results for National Security Systems. The expected results of ST&E procedures for NSS assure that all technical, operational, and assurance controls are specified, implemented, operational, and consistent with the functional requirements of the control statement. Additional assurance requirements for NSS are contained in DOE M 205.1-4, *National Security System Manual*.

2. The ST&E Report. The ST&E Report portion of the C&A package documents the security control's effectiveness and degree of implementation and includes information on each test procedure. The ST&E Report includes the following information:

   a. The ST&E procedure(s) for each control.

   b. For Site and Type forms of accreditation, ST&E procedures to be used for future instantiations.

   c. The control(s) to which the procedure applies.

   d. Assessment method(s) used to assess/evaluate the control.

   e. The attributes (Attachment 1) of the ST&E procedures.

   f. The expected results of each test procedure.

   g. The actual results of each test procedure.

   h. Analysis and evaluation of ST&E procedure results:

      (1) ST&E procedure was passed - obtained the expected results.

(2) ST&E procedure failed - did not obtain the expected results. If the control could not be corrected or was not practical to correct, the Certification Agent includes a description of vulnerabilities resulting from the absence of the control to be used for updating the Risk Assessment in the C&A package.

TMR-21-3, Operating Unit ST&E Processes

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement ST&E 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.

ATTACHMENT 1

ASSESSMENT METHOD ATTRIBUTE DESCRIPTIONS

The following table provides a summary of the assessment method attributes and attribute values by TMR-1 information system impact level. Descriptions of the attribute values follow the table.

TABLE 1: ASSESSMENT METHOD ATTRIBUTES AND ATTRIBUTE VALUES BY IMPACT LEVEL

ASSESSMENT METHODS: Interview, Examine, Test		**INFORMATION SYSTEM IMPACT LEVEL**		
ATTRIBUTE	**VALUE**	**LOW**	**MODERATE**	**HIGH**
Depth (Interview and examine methods only)	Generalized	√	---	---
	Focused	---	√	---
	Comprehensive	---	---	√
Type (Test method only)	Functional (black-box)	√	√	√
	Penetration	√	√	√
	Structural (gray-box, white-box)	---	---	√
Coverage (All methods)	Categories and number of assessment objects determined by organizations in collaboration with assessors.	√	√	√

Assessment Method: Interview

The Depth attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: (i) generalized; (ii) focused; and (iii) comprehensive.

- Generalized interviews consist of broad, high-level discussions with selected organizational personnel on particular topics relating to the security controls being assessed. This type of interview is typically conducted using a set of generalized, high-level questions and is intended to capture a broad, general understanding of the fundamental concepts associated with specifications, mechanisms, or activities.

- Focused interviews consist of broad, high-level discussions and more detailed discussions in specific areas with selected organizational personnel on particular topics relating to the security controls being assessed. This type of interview is typically conducted using a set of generalized, high-level questions and a set of more detailed questions in specific areas where responses indicate a need for more detailed investigation and is intended to capture the specific understanding of the fundamental concepts associated with specifications, mechanisms, or activities.

- Comprehensive interviews consist of broad, high-level discussions and more detailed, probing discussions in specific areas with selected organizational personnel on particular topics relating to the security controls being assessed (including the results of other assessment methods). This type of interview is typically conducted using a set of generalized, high-level questions and a set of more detailed, probing questions

in specific areas where responses indicate a need for more detailed investigation or where assessment evidence allows and is intended to capture the specific understanding of the fundamental concepts and implementation details associated with specifications, mechanisms, or activities.

The Coverage attribute addresses the categories of individuals to be interviewed (by organizational roles and associated responsibilities) and the number of individuals to be interviewed (by category). Organizations, in collaboration with information system assessors, determine the specific categories and numbers of individuals to be interviewed during the assessment process.

Assessment Method: Examine

The Depth attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: (i) generalized; (ii) focused; and (iii) comprehensive.

- Generalized examinations consist of brief, high-level reviews, observations, or inspections of security controls using a limited body of evidence or documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities.

- Focused examinations consist of detailed analyses of security controls using a substantial body of evidence or documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities, and where appropriate, high-level design information.

- Comprehensive examinations consist of detailed and thorough analyses of security controls using an extensive body of evidence or documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities, and where appropriate, high-level design, low-level design, and implementation-related information (e.g., source code).

The Coverage attribute addresses the categories of specifications, mechanisms, or activities to be examined and the number of specifications, mechanisms, or activities to be examined (by category). Organizations, in collaboration with information system assessors, determine the specific categories and numbers of specifications, mechanisms, or activities to be assessed during the assessment process.

Assessment Method: Test

The Type attribute addresses the types of testing to be conducted. There are three possible values for the type attribute: (i) functional testing; (ii) penetration testing; and (iii) structural testing.

- Functional testing methodology assumes knowledge of the functional specifications, high-level design, and operating specifications of the item under assessment. Also known as “black box” testing.

- Penetration testing methodology utilizes assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, to attempt to circumvent the security features of an information system.

- Structural testing methodology assumes (some) explicit knowledge of the internal structure of the item under assessment (e.g., low-level design, source code implementation representation). Also known as “gray box” or “white box” testing.

The Coverage attribute addresses the categories of mechanisms or activities to be tested and the number of mechanisms or activities to be tested (by category). Organizations, in collaboration with information system assessors, determine the specific categories and numbers of mechanisms or activities to be assessed during the assessment process. For mechanism-related testing that involves software, the coverage attribute also addresses the extent of the testing conducted (e.g., number of test cases, number of modules tested, etc.).