

**U.S. Department of Energy
Cyber Security Program**

**SECURITY TESTING
GUIDANCE**



January 2007

***This Guidance document was
developed and issued outside of the
Departmental Directives Program.***

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides Security Test and Evaluation (ST&E) guidance to assure the controls have been implemented correctly, function as described in the System Security Plan (SSP), produce the desired outcome in meeting the system's security requirements, and provide evidence that the controls have sufficient strength. ST&E results are reported as part of the Certification and Accreditation (C&A) package described in DOE CIO Guidance CS-2, *Certification and Accreditation Guide*.

The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE CIO (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

This Guidance is provided to Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-4, *National Security Systems Controls Manual* in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to assessing common and system specific controls during the C&A process. This Guidance also addresses testing and evaluation criteria in DOE CIO Guidance CS-2, *Certification and Accreditation Guidance*, and DOE CIO Guidance CS-3, *Risk Management Guidance*.

The National Institute for Science and Technology (NIST) Special Publication (SP) 800-53A (DRAFT), *Guide for Assessing the Security Controls in Federal Information Systems*, dated April 2006, may be used as a supplement for developing the Senior DOE Management PCSP and any related operating unit documentation required by the PCSP.

3. CANCELLATIONS.

None.

4. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-37 is Applicable*.

Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units, and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.
- c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM)*; the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot address all of the criteria by the scheduled milestone, DOE expects Senior DOE Management to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSP.

6. CRITERIA.

- a. Program Cyber Security Plan. Senior DOE Management PCSPs must comply with the criteria in DOE CIO Guidance CS-1, *Management, Operational, and*

Technical Controls Guidance, DOE CIO Guidance CS-2, *Certification and Accreditation Guide*, DOE CIO Guidance CS-3, *Risk Management Guidance*, and DOE Manual 205.1-4, *National Security Systems Controls Manual*. Senior DOE Management PCSPs must direct operating units to develop, document, and implement ST&E policies and procedures for the following criteria and commensurate with the level of security required for the organization's environment and specific needs.

- (1) All controls identified in each SSP are to be subjected to assessment procedure(s), during the Certification and Accreditation process described in DOE CIO Guidance CS-2, *Certification and Accreditation Guide*, that 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 instantiation (i.e., installation) of a system must be subjected to an ST&E process.
 - i. The accreditation of additional instantiations (i.e., additional identical installations) may be based on a subset of the ST&E procedures used for the first instantiation. This subset, which is approved by the Designated Approving Authority (DAA), must provide for overall assurance that future instantiations are implemented identically to the first instantiation.
 - ii. 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.
- (2) 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. The attributes of depth, coverage, and type must be reflected in each ST&E procedure as described in Attachment 2. The following assessment methods can be used.
 - (a) Interview: Focused discussions with individuals or groups to facilitate understanding, achieve clarification, or obtain evidence.
 - (b) Examine: Checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
 - (c) Test: Exercising one or more assessment objects under specific conditions to compare actual with expected behavior.

- (3) Each test procedure must identify expected results. 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.

(a) Low impact.

- i. The security control is in effect and meets explicitly identified functional requirements in the control statement.
- ii. The control is in place, no obvious errors exist, and, as flaws are discovered, they are addressed in a timely manner.

(b) Moderate impact.

- i. The security control is in effect and meets explicitly identified functional requirements in the control statement.
- ii. The System Security Plan (SSP) provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control 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.
- iii. To ensure correct implementation and operation, each control incorporates specific capabilities and/or produces specific documentation.
- iv. There are no obvious errors in the security control and it is implemented correctly and operating as intended.

(c) High impact.

- i. The security control is in effect and meets explicitly identified functional requirements in the control statement.
- ii. 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.
- iii. The developer/implementer is expected provide the design, development, implementation, and component/ integration testing of the controls and to produce associated design and implementation documentation to support these activities.
 - iv. There are no obvious errors in the control, that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and there is continuous improvement in security control effectiveness.
- (4) The ST&E procedures must be approved by the DAA prior to the beginning of the ST&E process. The Certification Agent and DAA may specify additional ST&E processes as part of their C&A activities.
 - (5) Test personnel are approved by the Certification Agent as being knowledgeable and qualified to perform the ST&E functions.
 - (6) The ST&E Report portion of the C&A package, identified in DOE CIO Guidance CS-2, *Certification and Accreditation Guide*, documents the security control's effectiveness and degree of implementation. The ST&E Report portion of the C&A package includes information on each test procedure. The ST&E Report includes the following information:
 - (a) The ST&E procedure(s) for each control.
 - (b) The control(s) to which the procedure applies.
 - (c) Assessment method(s) used to assess/evaluate the control.
 - (d) The attributes of the ST&E procedures.
 - (e) The expected results of each test procedure.
 - (f) The actual results of each test procedure.
 - (g) Analysis and evaluation of ST&E procedures results:
 - i. ST&E procedure was passed - obtained the expected results.
 - ii. 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 and an updated Risk Assessment in the C&A package.

- (7) 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 systems after the first system are to reference the system accreditation date and SSP under which the control was first evaluated.
- b. Criteria Unique to National Security Systems (NSS). Senior DOE Management PCSPs are to direct operating units to develop, document, and implement ST&E policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs. Senior DOE Management PCSPs are to require operating units to define and document the following:
 - (1) The ST&E procedures must associate each control described in the SSP with specific procedure(s) used to assess each control. Each ST&E procedure, as 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.
 - (2) The ST&E procedure identifies the assessment method (interview, examine, test) used to evaluate each control. The ST&E procedures must address which of the following additional attributes, as described in DOE M 205.1-4, *National Security Systems Controls Manual*, are accomplished by the assessment procedures
 - (a) For NSS where the Confidentiality Consequence of Loss (CoL) is Medium, the ST&E process should focus on the control being in place, performing the functional requirements detailed in the SSP, and being operational with no obvious errors.
 - (b) For NSS where the Confidentiality CoL is High, the ST&E process should focus 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.
 - (c) For NSS where the Confidentiality CoL is Very High, the ST&E process should focus 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 further 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.

- (3) Each ST&E procedure identifies the expected results of conducting the test. The expected results of ST&E procedures must 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 Systems Controls Manual*.
- c. ST&E Processes Documentation. The Senior DOE Management PCSP is to incorporate processes and procedures to accomplish ST&E documentation.
- (1) ST&E activities are described to include the depth, type, and coverage of ST&E based on the Security Category of the system to achieve the necessary level of assurance.
 - (2) Description of any ST&E report format.

7. REFERENCES.

The following national standards and guidelines provide relevant processes and procedures for implementing this Guidance.

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003

NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.

Other references are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

8. DEFINITIONS.

Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

SECURITY CATEGORY. The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on

organizational operations, organizational assets, or individuals. Security categories are defined in FIPS 199.

9. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE
CIO GUIDANCE CS-37 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2ASSESSMENT METHOD ATTRIBUTE DESCRIPTIONS

The following table provides a summary of the assessment method attributes and attribute values by FIPS 199 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.).