DOE CIO Guidance CS-8

Department of Energy

Cyber Security Program

CONFIGURATION MANAGEMENT GUIDANCE

November 2006

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 assistance in implementing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklist Users and Developers,*; and other applicable Departmental and Federal Information Systems security laws and regulations.

Configuration Management (CM) applies administration, technical direction, and surveillance to identify and document functional and physical characteristics of a configuration item, control changes, record and report change processing and implementation, and verify compliance with specified requirements. CM ensures the protection features approved for information system security are implemented and maintained by applying discipline and control to the implementation and operations of systems and the processes of system maintenance and modification. This Guidance offers a unified and consistent approach to be addressed by Senior DOE Management Program Cyber Security Plans (PCSPs).

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 Chief Information Officer (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, Operations, and Technical Controls Guidance* and DOE Manual 205.1-X, *National Security Systems Controls Manual*, in their PCSPs. Specifically, this Guidance applies to the Configuration Management Operational Controls in CS-1 and the Configuration Management Assurance Controls in the Manual.

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-8 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 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.. NIST 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, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance in their PCSPs.

6. CRITERIA.

a. Program Cyber Security Plans. Senior DOE Management PCSPs are to be consistent with the criteria in DOE CIO Guidance CS-1, *Management,*

Operational, and Technical Controls Guidance, and DOE Manual 205.1-X, *National Security Systems Controls Manual*. The PCSP is to include formal, documented processes to facilitate implementation of Senior DOE Management configuration management policy and associated configuration management controls (i.e., approved Minimum Security Configurations) for all information systems in all Senior DOE Management operating units.

To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement configuration management policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.

(1) Policy and processes for security configuration management for each information system.

(a) Develop a Configuration Management Plan (CMP) that defines the methodology for configuration change control during system development, tracking of security flaws, authorization of changes, and the Certification and Accreditation process. The CMP is to include at least the following:

i. Information system and configuration item unique identification and labeling;

ii. Design documentation, including system specification and configuration item specification(s);

iii. Implementation, maintenance, and monitoring of Minimum Security Configurations;

iv. Configuration change identification, tracking, control, and history;

v. Configuration status accounting to track changes from identification to implementation to produce a new baseline;

vi. Security configuration checklist for operating system software, application software, and hardware platforms;

vii. Configuration auditing to trace modifications to configuration items for authorized changes;

viii. Integration of vulnerability and patch management processes;

ix. Documentation of configuration change control methodology and tools used; and

x. Documentation of the methodology and tools used to monitor configuration changes.

(b) Develop monitoring processes for the documentation, control, and approval of configuration changes to all National Security Systems and other information systems in Security Categories Moderate and High.

(2) Minimum Security Configurations

(a) Minimum Security Configurations must be selected from recognized sources of checklist-producing organizations, including NIST[1], the National Security Agency (NSA)[2], the Security Technical Implementation Guides (STIGs) produced by the Defense Information Systems Agency (DISA)[3], and the Center for Internet Security (CIS) benchmarks[4].

(b) Specify Minimum Security Configurations for all information technology procurements.

(c) Minimum Security Configurations must be defined in the PCSP. Modifications to Minimum Security Configurations developed by the recognized sources must be fully documented in the PCSP.

(d) If an information system cannot implement a Minimum Security Configuration defined in the PCSP due to operational or mission requirements, a new Minimum Security Configuration is to be developed and approved by Senior DOE Management and documented in the SSP.

(3) Policy and processes for definition, implementation, maintenance, and monitoring of Senior DOE Management-approved Minimum Security Configurations for all information systems.

(a) Develop policies to ensure the Minimum Security Configurations specified in approved System Security Plans (SSPs) are implemented and maintained in each instantiation of system components by applying discipline and control to the processes of system maintenance and modification.

(b) Develop and deploy processes to detect any changes in system hardware, software, and firmware components that will modify or deviate from the approved Minimum Security Configuration of the SSP or the level of risk accepted by the DAA.

---

[1] The NIST checklist repository is located at http://checklists.nist.gov/.

[2] The NSA's checklists are available at http://www.nsa.gov/ia/.

[3] DISA's STIGs are available at http://iase.disa.mil/stigs/index.html.

[4] CIS's site is http://www.cisecurity.org/.

(4) Implement Configuration Management controls based on Security Categorization. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, is used to determine the security categorization of unclassified information/ information system. DOE Manual 205.1-X, *National Security Systems Controls Manual*, is used to categorize National Security Systems.

b. Configuration Management Processes/ Documentation. The Senior DOE Management PCSP is to incorporate processes, procedures, and documentation for performing risk-based Configuration Management to include at least the following:

(1) Documentation to include SSPs, Contingency Plans, user and administrator guidance, test plans, test procedures, and test results and

(2) Identification of the roles and responsibilities for change approval/ disapproval to establish a new baseline.

7. REFERENCES.

References are listed in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

8. DEFINITIONS.

Definitions specific to this Guidance are included in Attachment 2. Acronyms and terms applicable to DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

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-8 IS APPLICABLE

Office of the Secretary
Chief Information Officer
Departmental Representative to the Defense Nuclear Facilities Safety Board
Energy Information Administration
National Nuclear Security Administration
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
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 Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation and Chief Financial Officer
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of the Inspector General
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

DEFINITIONS

Baseline. A baseline is a set of critical observations or data used for a comparison or a control. A baseline indicates a cutoff point in the design and development of a configuration item beyond which configuration does not evolve without undergoing strict configuration control policies and procedures.

Configuration. Functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.

Configuration Accounting. The recording and reporting of configuration item descriptions and all departures from the baseline during design and production.

Configuration Audit. An independent review of computer software for the purpose of assessing compliance with established requirements, standards, and baselines.

Configuration Control. The process of controlling modifications to the system's design, hardware, firmware, software, and documentation (including operational (administrator manuals/ checklist, etc.) and security documents (SSP, etc) which provides sufficient assurance the system is protected against the introduction of improper modification prior to, during, and after system implementation.

Configuration Item. The smallest component of hardware, software, firmware, documentation, or any of its discrete portions, of a system which is tracked by the configuration management process.

Control. An element of configuration management consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.

Identification. An element of configuration management consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation.

Item. An aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process.

Security Category. A characterization of the information/ information system based on the consequence of loss of confidentiality, integrity, and/or availability of the information/ information system.

System Life-cycle. The period of time that begins when a system is conceived and ends when the system is no longer available for use. It usually includes the following phases: definition/initiation, design/development, implementation/integration, installation/operation, and disposal.