

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

**INTERCONNECTION AGREEMENTS
GUIDANCE**



July 28, 2006

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides guidance for the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Systems*, for interconnected information systems within the DOE, including the National Nuclear Security Administration (NNSA).

The DOE CIO will review this guidance annually and update it as necessary. Senior DOE Management and their 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 CIO Guidance CS-22, *National Security Systems Controls Guidance*, in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to controls AC-4 and CA-3 in CS-1 and ENV-INT.1 in CS-22.

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-5 is Applicable*.

Further, 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) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called 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 must address this guidance for all systems hosting unclassified 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*, provides 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. 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; DOE CIO Guidance CS-22, *National Security Systems Controls Guidance*; and NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provide 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 Program Cyber Security Plans (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 are to establish a Plan of Actions and Milestones for implementation of this Guidance into their PCSPs.

6. CRITERIA.

- a. Program Cyber Security Plans. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE CIO Guidance CS-22, *National Security Systems Controls*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement interconnection agreement 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 address the following.
 - (1) Processes and procedures for planning, documenting, and managing system interconnections to include–
 - (a) Purpose of the interconnection, such as types of services to be provided through the interface, types of information allowed to flow over the interface, and method of data exchange.

- (b) Baseline configuration of the interface, such as identification of hardware specifications, identification of protocols, identification of data formats, identification of allowed services, and identification of systems authorized to communicate over the interface by network address/ Domain Name Service name.
 - (c) Identification of methods to meet the security requirements of the interconnected systems and/ or adjudicate security implementation differences (e.g. clearances information protection methods, etc.) between interconnected systems.
 - (d) Identification of personnel authorized to approve the interconnection.
 - (e) Responsibilities and processes for mutual configuration management and change notification for the interface.
 - (f) Responsibilities and processes for mutual maintenance and operation of the interface.
 - (g) Responsibilities, processes, and methods for mutual incident response and reporting to include attacks and interface component failures.
 - (h) Responsibilities and processes for establishing cross-domain accounts.
- (2) Processes governing the creation and approval of Interconnection Agreements.
 - (3) The responsibilities relating to interconnection of information systems of the roles in the certification and accreditation (C&A) process.
 - (4) Criteria and processes for obtaining approval for the interconnection of information systems.

7. REFERENCES.

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

8. DEFINITIONS.

Definitions specific to this guidance are included in Attachment 2. Acronyms and terms applicable to all 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-5 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 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, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

GLOSSARY

Interconnection Agreement: An agreement established between organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

System Interconnection. The connection of two or more information systems and/or networks for the purpose of sharing data or other resources.