

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

**PASSWORD MANAGEMENT
GUIDANCE**



June 30, 2006

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides direction for the generation, protection, and use of passwords when they are used to support authentication for access to National Security and unclassified information systems within the DOE, including the National Nuclear Security Administration (NNSA).

This Guidance provides additional information to Senior DOE Management for addressing the controls related to authentication and the use of passwords in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance (Identification and Authentication)* and DOE CIO Guidance CS-22, *National Security Systems Controls Guidance*, in their Program Cyber Security Plans (PCSPs).

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. CANCELLATIONS.

None.

3. 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-12 is Applicable*.

Further, 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) may specify 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 are to 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*, provide additional information for identifying unclassified information requiring protection.

- d. National Security Systems. Senior DOE Management Program Cyber Security Plans (PCSPs) are to address this Guidance, Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program, the requirements of the *National Industrial Security Program Operating Manual (NISPOM)*, and DOE M 471.2-2, *Classified Information Systems Security Manual*, for all National Security systems. The 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.

4. 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&Ms) for implementation of this Guidance into their PCSP.

5. 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*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement password 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. Such policies must address the criteria in this Guidance for all National Security and unclassified DOE information systems, desktops, and laptops—excluding those information systems intended to provide unrestricted public access (e.g., public web servers)—that use a password mechanism to authenticate the identity of each person accessing the information system.
- b. Password Generation and Verification.
 - (1) Develop and implement a plan, including schedule and milestones, to eliminate the use of clear text reusable passwords in all operating unit information systems.
 - (2) Ensure passwords for servers, mainframes, telecommunications devices (such as routers and switches), and devices used for cyber security functions (such as firewalls, intrusion detection, and audit logging) are encrypted when stored electronically.
 - (3) Document in System Security Plans (SSPs) for legacy systems that do not have the technical capability to encrypt passwords, protection measures to mitigate the risks associated with maintaining clear text passwords.

- (4) Develop and implement a plan, including schedule and milestones, to eliminate weak password encryption algorithms (e.g., Windows LANMAN).
- (5) Document in SSPs for legacy systems that do not have the technical capability to eliminate weak passwords encryption algorithms the protection measures to mitigate the risks associated with maintaining weak password encryption.
- (6) Develop and implement a plan, including schedule and milestones, to eliminate the use of common or shared passwords among system and database administrators and shared local administrator accounts.
- (7) Document in SSPs for information systems where group passwords or shared local administrator accounts must be used for operational reasons, protection measures to mitigate the risks associated with using group passwords and shared accounts.
- (8) Ensure information systems using passwords to authenticate users do not display or print passwords as they are entered.
- (9) Ensure passwords are not communicated or distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.
- (10) Implement a mandatory two-factor authentication process for systems where passwords are used as one authentication method to access accounts with special privileges (e.g., system administrators).
- (11) Ensure all purchased or developed password generation and verification software generates passwords in accordance with either the criteria in Paragraph (a) below, a passphrase as described in Paragraph (b), or an entropy-based methodology as described in Paragraph (c) as follows.
 - (a) Non-entropy Password Generation Criteria.
 - i. Passwords contain at least eight non-blank characters.
 - ii. Passwords contain a combination of letters, numbers, and at least one special character within the first seven positions.
 - iii. Passwords contain a nonnumeric in the first and last position.
 - iv. Passwords do not contain the user ID.
 - v. Passwords do not contain any common English dictionary word, spelled forward or backwards (except words of three or fewer characters); dictionaries for other languages should also be used if justified by risk and cost benefit analysis as allowed by the applicable Senior DOE Management PCSP.
 - vi. Passwords do not employ common names.

- vii. Passwords do not contain any commonly used numbers (e.g., the employee serial number, Social Security number, birth date, phone number) associated with the user of the password.
- viii. Passwords do not contain any simple pattern of letters or numbers, such as “qwertyxx” or “xyz123xx.”

(b) PassPhrase

- i. Passphrases must contain 25 or more characters and at least 2 special characters.
- ii. Passphrases must not begin or end with a special character.

(c) Entropy-Based Password Generation

Password generation based on an entropy approach must comply with the guidance for a Level 1 Authentication Mechanism as described in NIST SP 800-63, *Electronic Authentication Guideline*.

c. User-created Passwords.

- (1) Prohibit the use of user-created passwords on National Security information systems in accordance with DOE M 471.2-2, *Classified Information System Security Manual*.
- (2) In those cases where the user creates his/her own password (regardless of whether said password is verified by password verification software), to ensure, through verification software or user training, that the selected password is consistent with the criteria in section 5.b.11 (a) above and is different than the passwords employed on his/her National Security systems.

d. Password Protection. Provide training, education, and awareness programs to instruct individuals to not –

- (1) Share passwords except in emergency circumstances or when there is an overriding operational necessity, as allowed in the information SSP. Once shared, passwords must be changed immediately after use.
- (2) Use group passwords (i.e., a single password used by a group of users) without some other mechanism that can assure accountability (such as separate and unique network User IDs).
- (3) Share group passwords outside the group of authorized users. Group passwords must be changed when any individual in the group is no longer authorized to access the information system where the group password is used. Group passwords must never be re-used.

- (4) Leave clear-text passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password.
 - (5) Enable applications to retain passwords for subsequent reuse.
- e. Password Changing. Ensure that passwords are changed—
- (1) from vendor-supplied passwords prior to first operational use or connection to a network;
 - (2) at least every 6 months;
 - (3) immediately after sharing;
 - (4) immediately, if operationally possible, but no longer than 1 business day after a password has been compromised, or after one suspects that a password has been compromised; and
 - (5) on direction from management.
- f. Administration. If the capability exists in the information system, application, or resource, configure the system to ensure the following:
- (1) Three consecutive failed attempts to provide a legitimate password for an access request results in an access lockout.
 - (2) Any password file or database employed by the information system is protected from access by unauthorized individuals.
 - (3) Definition of the criteria, including review of the need for continuing information system access, for restoring access to an information system after access lockout or password expiration.
 - (4) When a password does not comply with those requirements of Paragraph 5.b, and if the failure to comply is verifiable, then the password is rejected.
 - (5) Individuals are notified that their passwords will expire after 6 months and must be changed to continue access to the information system or lockout will occur.

6. REFERENCES.

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

7. DEFINITIONS.

Definitions specific to this Guidance are defined 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*.

8. 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-12 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
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

DEFINITIONS

Passphrase. A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer.

Reusable Password. A data item associated with a user ID that remains constant, and is used for multiple access requests over some explicit time interval.

Special Character. Any non-alphanumeric character.