Cyber Security Technical and Management Requirements

Authenticator Management (TMR-11)
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). This TMR document provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

An effective authenticator management policy is critical to secure Department of Energy (DOE) information resources. This TMR establishes a risk-based approach to authenticator management that is to be covered in each PCSP for information systems within the DOE. It also provides for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*. Senior DOE Management may specify and implement additional requirements in the PCSP to address specific risks, vulnerabilities, or threats within its operating units.

Cancellations

This TMR replaces DOE CIO Guidance CS-12, *Password Management Guidance,* dated July 7, 2006.

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-11-1, Senior DOE Management Authenticator Management Policy

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing the requirements for authenticator management policies and procedures for all operating units, programs, and systems. The Senior DOE Management PCSP is to describe the authenticator management process to include the following:

1. Authenticator Generation and Verification.

   a. Eliminate clear text reusable passwords, encryption algorithms that are not FIPS 140-2 certified, and the use of common or shared passwords.

   b. Document in the System Security Plans (SSPs) for legacy systems that do not have the technical capability to encrypt passwords controls to mitigate the risks associated with maintaining clear text passwords and with maintaining weak password encryption.

   c. Document in SSPs for information systems where group passwords or shared local administrator accounts must be used for operational reasons controls to mitigate the risks associated with using group passwords and shared accounts.

   d. Ensure that passwords for servers, mainframes, desktops/ workstations, 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.

   e. Require the use of six-character passwords on Personal Digital Assistants (PDAs).

   f. Require the use of mandatory multi-factor authentication process for system administrator and privileged user access to systems where passwords are used as one authentication method.

   g. Ensure that authenticator generation and verification software generates passwords in accordance with either the criteria in Paragraph (1) below, a passphrase as described in Paragraph (2), or an entropy-based methodology as described in Paragraph (3) as follows:

      (1) Non-entropy Password Generation Criteria.

         (a) Passwords contain at least eight non-blank characters.

         (b) Passwords contain a combination of letters, numbers, and at least one special character within the first seven positions.

         (c) Passwords contain a nonnumeric in the first and last position.

         (d) Passwords do not contain the user identification (userid).

         (e) 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 Senior DOE Management PCSP.

(f) Passwords do not employ common names.

(g) 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.

(h) Passwords do not contain any simple pattern of letters or numbers, such as “qwertyxx” or “xyz123xx.”

(2) Passphrase Criteria

(a) Passphrases must contain 25 or more characters and at least 2 special characters.

(b) Passphrases must not begin or end with a special character.

(3) 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: Recommendations of the National Institute of Standards and Technology*.

(4) Passcodes (such as Personal Identification Numbers) are not required to comply with the password criteria.

h. Prohibit the use of user-created passwords on National Security Systems.

2. Authenticator Protection. Provide training, education, and awareness programs to instruct individuals to:

a. Ensure that created authenticators for unclassified information systems are consistent with the criteria in Paragraph 1.g. above.

b. Maintain unique authenticators (i.e., passphrases or passwords) for each National Security System for which they are authorized that are different from those utilized on unclassified information systems.

c. Not communicate or distribute authenticators through non-encrypted electronic mail, voice-mail, or left on answering machines

d. Not share authenticators except in emergency circumstances or when there is an overriding operational necessity, as allowed in the SSP. Once shared, passwords, passphrases, and oasscodes must be changed immediately after use.

e. Use group passwords (i.e., a single password used by a group of users) only with additional mechanism(s) that can assure accountability (such as separate and unique User IDs).

f. Not 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.

g. Secure clear-text authenticators in a location that is not accessible to others and where protection is equal to or more than that required for protecting the information that can be accessed using the authenticator.

h. Not enable applications to retain passwords, passphrases, or passcodes for subsequent reuse.

3. Password and Passphrase Changing. Ensure that passwords and passphrases are changed:

a. from those supplied by the vendor prior to first operational use or connection to a network;

b. at least every 6 months;

c. immediately after sharing;

d. immediately after an actual or suspected compromise; and

e. on direction from management.

4. Administration. If the capability exists in the information system, application, or resource, ensure that:

a. User-created authenticators on unclassified information systems are consistent with the criteria in Paragraph 1.g. above.

b. User-created authenticators on unclassified information systems are different from those employed by the same user on National Security Systems.

c. Passwords and passphrases that do not comply with requirements of Paragraph 1.g. above are rejected.

d. Prior to the expiration date, users are notified that their passwords/passcodes will expire and must be changed to continue access to the information system or lockout will occur.

TMR-11-2, Operating Unit Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement policies and procedures for authenticator management compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization’s environment and specific needs.