

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 01/23/2013)

- Subject:** Security Awareness and Cyber Security Training Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish specific criteria for the identification of individuals with access to Critical Cyber Assets (CCA) and requirements for the quarterly security awareness and annual cyber security training of those individuals with such access pursuant to compliance with the Critical Infrastructure Protection (CIP) Reliability Standards of NERC and in support of the reliability of cyber systems supporting the bulk electric system (BES). The benefit of this Directive and Standard (D&S) is that it promotes compliance with the CIP Reliability Standards of NERC.
- Authority:** The Reclamation Act of 1902 (Act of June 17, 1902, ch. 1093; 32 Stat. 388), the Town Sites and Power Development Act of 1906 (Act of April 16, 1906, ch. 1361, 34 Stat. 116), Federal Power Act of 1920 (Act of June 10, 1920, ch. 285, 41 Stat. 1063), Reclamation Project Act of 1939 (Act of August 4, 1939, ch. 418, 53 Stat. 1187), Energy Policy Act of 1992 (Act of October 24, 1992, 106 Stat. 2776), Energy Policy Act of 2005 (Act of August 8, 2005, 119 Stat. 594), acts relating to individual dams or projects, and Federal Energy Regulatory Commission approved NERC Reliability Standards (18 CFR Part 40).
- Approving Official:** Director, Information Resources Office (IRO)
- Contact:** IRO, 84-21000
Security, Safety, and Law Enforcement (SSLE), 84-40000
Policy and Administration, Human Resources Division, 84-58000
-

1. **Introduction.** The NERC CIP Standards establish annual cyber security training and quarterly security awareness requirements designed to reduce the risk that individuals with unescorted physical and/or logical access to CCA pose to those assets as a result of their cyber-related behavior or actions. This D&S establishes requirements and criteria to support the Bureau of Reclamation's quarterly security awareness and annual cyber security training activities.
2. **Applicability.** This D&S applies to all personnel, contractors, vendors, operating partner personnel, temporary staff, and visitors who will be permitted unescorted access to Reclamation's CCA.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 01/23/2013)

3. **Definitions.**

- A. **BES.** The electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.
- B. **Critical Assets.** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.
- C. **CCA.** A cyber asset, including programmable electronic devices, communication networks, hardware, software, and data that is essential to the reliable operation of a CA.
- D. **Cyber Security Training.** Training provided to personnel to establish and/or improve the individual's skills or knowledge with respect to cyber security as applied to CCA.
- E. **Directorate.** The organizational component of a Director. This includes the Director, Technical Resources; regional directors; Director, SSLE; Director, Policy and Administration; and Director, IRO.
- F. **Directors.** Reclamation Senior Executives responsible for specific programs or facilities. This definition includes: the Director, Technical Resources; regional directors; Director, SSLE; Director, Policy and Administration; and Director, IRO.
- G. **Personnel Risk Assessment.** An assessment, completed by Reclamation, of organizational risk related to the access (either unescorted physical access or logical access) granted to an individual based on verification of their identity and completion of a 7-year criminal history check – specifically, a Special Agency Check or other criminal history check as provided by the Office of Personnel Management.
- H. **Qualifying Individual.** A Reclamation employee, contractor, vendor, operating partner's employee, temporary staff member, or visitor who will be permitted logical and/or unescorted physical access to Reclamation's CCA. This also includes all individuals who have logical and/or unescorted physical access to cyber systems that provide for the physical protection of CCA.
- I. **Quarterly Security Awareness.** Information, guidance, or reminders periodically provided to personnel for reinforcement in sound security practices.
- J. **Regional Reliability Organization.** An entity within NERC that ensures that a defined regional area of the BES is reliable, adequate, and secure.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 01/23/2013)

K. **Unescorted Access.** Access, specifically physical access, to CCA where such access is not monitored by a designated individual who maintains awareness of what the escorted individual is doing at all times during the duration of the physical access. All logical access to CCA is considered unescorted.

4. **Responsibilities.**

A. **Policy and Administration, Chief, Human Resources Division.** The Chief, Human Resources Division will support the delivery and documentation of annual cyber security training, including support for the coordination of efforts to make the training described in Paragraph 5.B., below, available through the Department of the Interior's Learning Management System (DOILearn). The Chief, Human Resources Division will also establish processes, as necessary, to support the entry of information recording cyber security training completions for all persons with unescorted access to CCA (including persons that are not Reclamation employees).

B. **Technical Resources, Senior Advisor, Hydropower.** The Senior Advisor, Hydropower administers the Electric Reliability Compliance Program. Working with all responsible directors, the Senior Advisor, Hydropower certifies Reliability Standards' compliance, as applicable, to NERC and Western Electricity Coordinating Council (WECC).

C. **Director, IRO.** The Director, IRO is identified as Reclamation's Senior Manager with overall responsibility for leading and managing the implementation and adherence to the NERC CIP Standards, CIP-002 through CIP-009. The Director, IRO is also responsible for the coordination of efforts to prepare and deliver quarterly security awareness and annual cyber security training materials in accordance with Paragraph 5.A. below. The Director, IRO will perform annual reviews of the cyber security training materials. All awareness and training efforts shall be coordinated with the Director, SSLE to ensure appropriate security training coverage.

D. **Director, SSLE.** The Director, SSLE is responsible for the preparation of physical security materials and aids as necessary to promote and support Reclamation's quarterly security awareness and annual cyber security training efforts.

E. **Directors.** Each Director is responsible for the execution and documentation of all applicable NERC and WECC compliance activities, including the support and coordination of information technology related compliance requirements with the IRO. This includes the necessary collection of information as needed to support the identification of personnel, contractors, vendors, partner employees, temporary staff, and visitors requiring access to CCA over which the directorate has oversight.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 01/23/2013)

- F. **Reliability Compliance Representative.** As required in Reclamation Manual Policy, *North American Electric Reliability Corporation (NERC) Electric Reliability Standard Compliance (FAC P13)*, each directorate is represented by a reliability compliance representative who is responsible for coordinating directorate compliance-related matters with the Power Resources Office and other directorates. Unless otherwise indicated and documented by the directorate, the reliability compliance representative is responsible for coordinating directorate training needs, procedures, information submittals, completions, and records retention as necessary to support NERC CIP compliance reporting. This includes the maintenance and retention of records supporting the distribution of quarterly security awareness and the completion of annual cyber security training.
- G. **Area and Facility Managers.** Area and facility managers responsible for identified Reclamation CCA are responsible and accountable for controlling access to their CCA (including escorted access) and for performing and documenting activities associated with the identification of training candidates and their completion of required quarterly security awareness and annual cyber security training within the area or facility office to attain and maintain compliance with this D&S.
- H. **Regional Training Offices.** The required cyber security training, defined in this D&S, will be assigned to the learning plans of targeted individuals by regional training offices. Regional training offices are further responsible for ensuring that cyber security training completions for all personnel with unescorted access to CCA are recorded in DOI Learn in accordance with procedures outlined by the Chief, Human Resources Division in Denver.

5. **Procedures.**

- A. **Quarterly Security Awareness.** Quarterly security awareness shall be delivered to all Qualifying Individuals through the reliability compliance representatives (or the designated regional coordinator, per Paragraph 4.F.) The Office of the IRO will furnish the representatives (or coordinators) with awareness materials on a quarterly basis. Should the region elect to use other awareness materials, a copy of the delivered awareness material(s) must be locally maintained. Records related to the delivery of quarterly security awareness materials shall be maintained in accordance with Paragraph 5.F., below. Quarterly security awareness shall be delivered to Qualifying Individuals via any of the following:

- (1) a direct communication to the qualifying individual in the form of an email message, memorandum, or requirement to complete additional specified training;
- or

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 01/23/2013)

- (2) an indirect communication to the qualifying individuals in the form of a poster, flier, brochure, or log-on banner; or
 - (3) any other mechanism that may be deemed appropriate by management to remind qualifying individuals of their responsibilities with respect to the observance of sound security practices.
- B. Cyber Security Training Requirements and Annual Reviews.** Cyber security training completed to address the requirements of this D&S, including policies, access controls, and procedures for CCA, shall be performed via the presentation entitled “*Cyber Security Training: Supporting North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards.*” All individuals who qualify for training under this D&S must annually complete the training. Course content must address items appropriate to personnel roles and responsibilities including the access to and use of CCA recovery and/or reestablishment plans following a Cyber Security Incident; the proper use of CCA; physical and/or electronic access controls; and handling requirements for CCA or CCA information. All cyber security training will be reviewed annually and will be updated when necessary.
- C. Training Requirements for Unescorted Access.** Except where otherwise specifically permitted in companion D&S, no individuals shall be afforded unescorted access to CCA prior to having successfully completed cyber security training in accordance with Paragraph 5.B., above.
- D. Reciprocal Training Agreements.** In instances where a partner entity must be provided access to Reclamation CCA in order to support the management or maintenance of that entity’s equipment or systems, area and facility managers may, in consultation with their directorate, establish reciprocal agreements that avoid the need for Reclamation to train the entity’s staff. Such agreements, if established, are subject to the following conditions:
- (1) the entity and their personnel with access to Reclamation CCA are subject to the NERC CIP Standards;
 - (2) the entity’s personnel are provided with both security awareness and cyber security training in accordance with the NERC CIP Standards and records of such awareness and training are available to Reclamation under the terms and conditions of the reciprocal agreement;
 - (3) a personnel risk assessment has been successfully adjudicated on the entity’s personnel, by either the entity or Reclamation,

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 01/23/2013)

- (4) Reclamation is provided access to the entity's cyber security training materials to ensure that they appropriately address NERC CIP security requirements to which Reclamation's cyber assets are subject; and
 - (5) the agreement is formally documented and signed by a directorate-level (or equivalent or delegate) representative of both Reclamation and the entity.
- E. **Training and Awareness Records.** All completed cyber security training supporting this D&S shall be recorded in DOI Learn. This includes the cyber security training supporting all individuals who will be permitted unescorted access to Reclamation's CCA. DOI Learn will serve as the official repository of cyber security training compliance records for Reclamation's NERC CIP Standards compliance efforts. Records demonstrating compliance with the distribution of quarterly security awareness materials to all Qualifying Individuals will be the responsibility of the regional directors through their reliability compliance representatives and regional training offices.
- F. **Retention of Training and Awareness Records.** Training and awareness records supporting the demonstration of compliance with this D&S shall be retained such that the current and prior full calendar year of training and awareness history is available for review or audit.
6. **Related D&S.** Related and supporting D&S, as well as overarching Policy, are available in the Information Resources Management (IRM) section of the Reclamation Manual.