

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Physical Security Plans Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish specific, Bureau of Reclamation-wide requirements and criteria supporting the preparation, implementation, maintenance, and approval of Physical Security Plans for the protection of Critical Cyber Assets (CCA) 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 improved compliance with the Critical Infrastructure Protection (CIP) Reliability Standards of NERC.
- Authority:** Reclamation Act of 1902 (June 17, 1902; ch. 1093; 32 Stat. 388); Town Sites and Power Development Act of 1906 (April 16, 1906; Pub. L. 59-103; 34 Stat. 116); Federal Water Power Act of 1920 (June 10, 1920; Pub. L. 66-280; 41 Stat. 1063); Reclamation Project Act of 1939 (August 4, 1939; Pub. L. 76-260; 53 Stat. 1187); Department of Energy Organization Act of 1977 (August 4, 1977; Pub. L. 95-91; 91 Stat. 565); Energy Policy Act of 1992 (October 24, 1992; Pub. L. 102-486; 106 Stat. 2776); Energy Policy Act of 2005 (August 8, 2005; Pub. L. 109-58; 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), 84-45000
-

1. **Introduction.** The NERC CIP Reliability Standards establish requirements for the physical protection of cyber assets associated with the control and monitoring of BES assets. The protection requirements are applicable to cyber assets based on the identification of those assets as either CCAs or cyber assets that have been grouped within an electronic security perimeter (ESP) with CCAs. This D&S establishes requirements and criteria supporting the preparation, implementation, maintenance, and approval of Physical Security Plans addressing the physical protection of cyber assets within an ESP.
2. **Applicability.** This D&S applies to directors, supervisors, and all staff responsible for the preparation, implementation, maintenance, and approval of Physical Security Plans supporting the protection of cyber assets subject to the NERC CIP Reliability Standards.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

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 Asset (CA).** 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. **Days.** Wherever used in this D&S, days refer to contiguous calendar days, including weekends and holidays.
- 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. **ESP.** The logical border surrounding a network to which CCAs are connected and for which access is controlled. All cyber assets and components internal to the ESP boundary, as well as all cyber assets and components which reside on the ESP boundary, are subject to the physical security requirements of this D&S, its companion D&S, and overarching Policy.
- H. **Physical Access Control System (PACS).** A cyber-based system that supports the protection, access control, and access monitoring of a physical security perimeter (PSP). PACS may also be referred to as Electronic Access Control and Surveillance System (EACSS) where those systems provide protection, access control, and access monitoring of one or more PSPs.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- I. **PSP.** A PSP is a physical, completely enclosed (“six wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which CCAs are housed and to which access is to be controlled. Breaks in the boundary are allowed for physical ingress/egress points.
 - J. **Reliability Standards.** Any of a number of NERC or Western Electricity Coordinating Council (WECC) Standards, the specific requirements of which are applicable to Reclamation and define tasks, procedures or conditions for maintaining the reliability of the BES. For purposes of this D&S, the specific Reliability Standards of concern include Standards CIP-002 through CIP-009, inclusive. Although CIP-001 is identifiable as a CIP Reliability Standard, it does not specifically address the Security of CCAs and is identified as outside the scope of this D&S. As used throughout this D&S, Standards CIP-002 through CIP-009 will be referred to collectively as the NERC CIP Reliability Standards.
4. **Responsibilities.**
- A. **Director, IRO.** The Director, IRO is identified as Reclamation’s single senior manager with overall responsibility for leading and managing the implementation and adherence to the NERC CIP Reliability Standards.
 - B. **Director, SSLE.** The Director, SSLE is responsible for the establishment, execution, and documentation of compliance measures supporting the physical protection measures identified in the NERC CIP Reliability Standards.
 - C. **Directors.** Each director with identified CCAs under their jurisdiction is responsible for the establishment, execution, and documentation of all NERC CIP compliance activities related to the physical security system plans and functionality within their directorate. This includes the preparation and review of documentation as necessary to support the physical security compliance reporting.
 - D. **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 the other directorates. Unless otherwise indicated and documented by the directorate, the reliability compliance representative is responsible for coordinating directorate Physical Security Plan preparation, implementation, maintenance, and approval and securing any certifications necessary to support final reporting.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- E. **Area and Facility Managers.** Area managers or facility managers are responsible for preparation, implementation, and maintenance of Physical Security Plans that document physical protection of CCA within the area or facility.
5. **Procedures.**
- A. **Prerequisites.** PSPs must be identified following the procedure outlined in Paragraph 5.B., once prerequisite information has been determined through a refinement process involving the following steps:
- (1) The identification of the CCAs shall be performed in accordance with Reclamation Manual TRMR D&S, *Critical Cyber Asset (CCA) Identification Supporting North American Electric Reliability Corporation (NERC) Reliability Compliance* (IRM TRMR-34).
 - (2) The identification of the ESPs must be performed in accordance with Reclamation Manual Temporary Reclamation Manual Releases (TRMR) D&S, *Electronic Security Perimeter (ESP) Identification Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-45).
- B. **Identification of PSPs.** Once necessary information regarding the location and extent of ESPs has been established, PSPs shall be identified as follows:
- (1) PSPs shall be established around all identified ESPs. Each identified ESP shall reside completely within a PSP.
 - (2) More than one ESP may reside within an established PSP.
 - (3) Physical access to the cyber assets located within the PSP shall be controlled, monitored, and logged at the ingress/egress points into and out of the PSP.
- C. **Physical Security Plans.** Physical Security Plans shall be developed for all PSPs identified under this D&S. A single Physical Security Plan may address more than one PSP, provided all PSPs covered by the Plan are clearly identified within the Plan. Physical Security Plans shall follow the outline and template presented in Appendix A. This outline/template will be maintained by Reclamation's SSLE office and will include requirements for information addressing compliance with the NERC CIP Reliability Standards. Additional information supporting the use of the Appendix A outline/template is provided in Appendix B.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- D. **Protection of Physical Access Control Systems and Data.** The Physical Security Plan must describe how cyber assets and associated data, that are components or descriptions of a PACS, are physically protected. For additional information, refer to Reclamation Manual Temporary Reclamation Manual Releases (TRMR) D&S, *Cyber Asset Access Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-42).
- E. **Monitoring and Logging of Physical Access.** The Physical Security Plan must document methods used to monitor and log physical access into a PSP. This includes monitoring and logging visitor access into a PSP as described in Appendix A. For additional information, refer to Reclamation Manual Temporary Reclamation Manual Releases (TRMR) D&S, *Cyber Asset Access Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-42).
- F. **Maintenance and Testing of PACS.** The Physical Security Plan must document methods and procedures for performing maintenance and testing of PACS to assure proper functionality. For additional information, refer to Reclamation Manual Temporary Reclamation Manual Releases (TRMR) D&S, *Cyber Asset Access Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-42).
- G. **Physical Security Plan Approval.** Based on the NERC CIP Standards, Reclamation's single senior manager, Director, IRO, must approve all physical security plans. Per this D&S, Reclamation physical security plans will be approved by the Regional Directors, or their delegate, with direct responsibility for implementation of those plans (this is not a formal delegation of authority).
- H. **Physical Security Plan Maintenance.** Any changes to the physical access control mechanisms, procedures, or processes (including redesigns, reconfigurations, or changes to the number or types of access points) must be documented in the Physical Security Plan within 30 days of the changes. Regardless of any changes to the physical control environment, the Physical Security Plan shall be reviewed annually to ensure it accurately represents the protected environment and enacted control mechanisms, processes, and procedures.
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.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

7. **Appendices.**

- A. **Appendix A.** Physical Security Plan (provided as an outline/template).
- B. **Appendix B.** Physical Security Plan Instructions.