

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Cyber Asset (CA) Security Vulnerability Assessment Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish specific, consistent requirements and procedures to perform electronic security perimeter (ESP), CCA, and non-CCA security assessments 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:** 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 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
-

1. **Introduction.** The NERC CIP Reliability Standards establish protection requirements that include periodic assessment of the security controls for CCA supporting the control and monitoring of BES assets. The protection requirements are applicable to cyber systems and cyber assets based on their identification as residing within an ESP and/or providing physical or logical protection to the ESP. This D&S establishes requirements and criteria to support annual security vulnerability assessments of security baselines for ESP access points and all cyber assets within an ESP.
2. **Applicability.** This D&S applies to Bureau of Reclamation directors, supervisors, and all staff responsible for planning and executing security vulnerability assessments for all ESPs established around cyber-based assets identified as CCA and security vulnerability assessments for all other cyber assets within the ESP.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

3. **Definitions.**

- A. **Access Controls.** Technical, operational, or management security controls, put in place at access points to reduce the risk that unauthorized access (either logical or physical) can be gained to cyber assets protected by the access controls.
- B. **Access Point.** A communications mechanism (port or communication line), exposed at the boundary of an ESP that provides logical access to cyber assets within the ESP.
- C. **BES.** As defined by NERC, 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.
- D. **Critical Asset (CA).** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES. Specific Reclamation assets have been identified as critical based on the criteria and procedures established by Reclamation Manual, IRM TRMR-10-1, Appendix A, *Critical Asset Identification Methodology: Pursuant to NERC Critical Infrastructure Protection (CIP) Standards*.
- E. **CCA.** CCAs are cyber assets, including programmable electronic devices, communication networks, hardware, software, and data that are essential to the reliable operation of CAs.
- F. **Directorate.** The organizational component of a Director. This includes the Director, Technical Resources; regional directors; Director, Security, Safety, and Law Enforcement (SSLE); and Director, IRO.
- G. **Directors.** Reclamation Senior Executives responsible for specific programs or facilities. This definition includes: the Director, Technical Resources; regional directors; Director, SSLE; and Director, IRO.
- H. **ESP.** An ESP is the logical border surrounding a network to which CCA 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 security requirements of this D&S, its companion D&S, and overarching policy.
- I. **Ports and Services.** The set of enabled ports and services used to transfer data based on a particular digital communications protocol (for example TCP/IP).

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- 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 which 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.
- K. **Security Vulnerability Assessment.** A systematic approach to identifying weaknesses in the logical protections that have been put in place.
4. **Responsibilities.**
- A. **Director, IRO.** The Director, IRO is Reclamation's single senior manager with overall responsibility for leading and managing implementation and adherence to the NERC CIP Reliability Standards. The Director, IRO is responsible for development of Reclamation Policy that includes requirements to support the performance of security vulnerability assessments.
- 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 WECC and advises the Deputy Commissioner for Operations on the status of Electric Reliability Compliance Program issues.
- C. **Directors.** Each director with identified CA under their jurisdiction is responsible for the establishment, execution and documentation of all compliance activities related to the CCA within their directorate including the completion of annual security vulnerability assessments.
- 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 other directorates. Unless otherwise

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

indicated and documented by the directorate, the reliability compliance representative, or his delegate, is responsible for coordinating directorate compliance planning, information submittals, and records as necessary to support NERC CIP compliance reporting.

- E. **Area and Facility Managers.** Area managers and facility managers are responsible for performance of security vulnerability assessments as described in this D&S within their area or facility office.

5. **Procedures.**

A. **Prerequisites.**

- (1) **Identification of CCA.** The identification of CCAs shall be performed as addressed in Reclamation Manual D&S, *Critical Cyber Asset (CCA) Identification Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-34).
- (2) **Identification of ESP.** ESP identification shall be performed to protect the identified CCA and must follow the procedure outlined in Reclamation Manual D&S describing procedures for ESP identification and protection to support NERC CIP Reliability Standard compliance.
- (3) **Identification of Security Baseline.** The security baseline configuration for each ESP access point and all cyber assets within an ESP must be established and shall be used as a reference for vulnerability assessment activities. For additional information on the security baseline refer to Reclamation Manual D&S, describing procedures for configuration management with procedures to perform ports and impact analysis testing to support NERC CIP Reliability Standard compliance.

- B. **Develop and Document Security Vulnerability Assessment Procedures.** The area manager or facility manager is responsible for the development of procedures to assess vulnerability. The security baseline configuration will be used as a benchmark, but the baseline may be revised as necessary to make sure system operational improvements, changes, or upgrades are made without any negative impacts on cyber security controls.

- C. **Perform Security Vulnerability Assessments.** For more details concerning the procedures for vulnerability assessments refer to Appendix A of this D&S, *Vulnerability Assessment Requirements*. Security vulnerability assessments shall be performed at least annually. Assessment documentation must show results of scans or other

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

assessment methods. The area or facility manager must develop and execute plans for mitigation of identified vulnerabilities. Vulnerability assessment documentation and the associated mitigation plans must be retained for the previous 3 calendar years.

6. **Related D&S.** Related and supporting D&S, as well as the overarching Policy, are available in the Information Resources Management (IRM) section of the Reclamation Manual.