

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Cyber Security Incident Response and Recovery Program Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish specific and consistent requirements and procedures for incident response and recovery planning associated with Critical Cyber Assets (CCA) pursuant to compliance with the Critical Infrastructure Protection (CIP) Reliability Standards of NERC for the benefit and in support of the protection and reliability of cyber systems supporting the bulk electric system (BES).
- Authority:** Computer Security Act of 1987 (January 8, 1988; Pub. L. 100-235); Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (October 30, 2000; Pub. L. 106-398; 114 Stat. 1654A-12) including Title X, Subtitle G, *Government Information Security Reform*; Energy Policy Act of 2005 (August 8, 2005; Pub. L. 109-58; 119 Stat. 594); Office of Management and Budget (OMB) Circular No. A-123, *Management Accountability and Control* (June 21, 1995; 31 U.S.C. § 3512); Federal Energy Regulatory Commission approved NERC Reliability Standards (18 CFR Part 40); OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (December 24, 1985; 50 Federal Register 52730; *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (January 2000); and Department of the Interior Departmental Manual Part 375, Chapter 19, *Information Technology Security*.
- Approving Official:** Director, Information Resources Office (IRO)
- Contact:** IRO, 84-21000
-

1. **Introduction.** The NERC CIP Standards establish incident reporting and response planning for all cyber assets to better support the defense of cyber-controlled and monitored BES assets from cyber-based security threats, vulnerabilities, and incidents. These incident and recovery reporting and planning requirements are in addition to current Bureau of Reclamation incident response procedures and reporting requirements. While the NERC specific requirements may be integrated into existing processes and procedures, they do not supersede any established requirements. Many of the established requirements can be found in: local standard operating procedures (SOPs); emergency action plans; *BOR Incident Response Standard Operating Procedure* (Incident Response SOP); Reclamation Manual Directives and Standards (D&S), *Emergency Notification System* (SLE 07-01), and *Power Operation and Maintenance Incident Evaluation and Reporting* (FAC TRMR-18).

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

2. **Applicability.** This D&S applies to directors, supervisors, and all staff responsible for incident reporting and recovery planning associated with cyber systems, cyber subsystems, and related cyber-based assets directly supporting Reclamation's power and power-related facilities that have been defined as critical assets (CA) per NERC Reliability Standards.

3. **Definitions.**
 - A. **BES.** As defined by the Regional Reliability Organization, 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. **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's *Critical Asset Identification Methodology: Pursuant to NERC Critical Infrastructure Protection (CIP) Standards*.

 - C. **CCA.** Cyber assets, including programmable electronic devices, communication networks, hardware, software, and data that are essential to the reliable operation of CAs.

 - D. **Electricity Sector Information Sharing and Analysis Center (ES-ISAC).** Operated by NERC, the ES-ISAC serves the electricity sector by facilitating communications between electricity sector entities, U.S., Canadian federal governments, and other critical infrastructure sectors.

 - E. **Incident.** Incidents are security events known to constitute a violation of law or policy or have led to the jeopardizing of infrastructure, facilities, personnel, or information.

 - F. **Incident Response.** Response to an incident involves preparation, detection, and analysis of a security event.

 - G. **Recovery.** Recovery will include all efforts to contain and remove a problem associated with the cyber asset system functionality. Recovery also includes the process of restoring failed components to their original functioning status prior to the incident.

 - H. **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

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

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 implementation and adherence to the NERC CIP Reliability Standards. The Director, IRO is responsible for reporting all appropriate incidents to the ES-ISAC.
- B. **Director, Security, Safety, and Law Enforcement (SSLE).** The Director, SSLE is responsible for all criminal investigations performed at Reclamation facilities.
- 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 planning and implementation of procedures to address incident response and recovery.
- D. **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 compliance as applicable to NERC and WECC and advises the Deputy Commissioner, Operations on the status of Electric Reliability Compliance Program issues.
- E. **Area and Facility Managers.** Area and facility managers are responsible for the development, maintenance, and implementation of the incident response plans and CCA recovery plans within the area or facility office. This involves proper training of local staff to identify and communicate security events, as well as, training to implement recovery plans.

5. **Procedures.**

- A. **Incident Response Planning.** An incident response plan must be developed by the facility or area manager that addresses the requirements list that follows. The *Incident Response SOP* must be used as appropriate to develop the incident response plan addressing the following requirements:

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (1) procedures to characterize and classify events as potential reportable incidents;
 - (2) roles and responsibilities, incident handling procedures, communication plans;
 - (3) notifying the Reclamation Enterprise Service Center (RESC) of any potential reportable cyber security incidents;
 - (4) process for updating the incident response plan within 30 days of change;
 - (5) process for incident response plan annual review; and
 - (6) process for incident response plan annual testing.
- B. Exercise the Incident Response Plan.** The incident response plan must be exercised annually. The plan may be exercised by performing a table top exercise, an operational exercise, or by performance of an actual response to an incident.
- C. Report Cyber Security Incidents.** Cyber security incidents must be reported to ES-ISAC via the reporting form that is located at <http://www.esisac.com/library-guidelines.htm>. The Director, IRO will determine which of the cyber security incidents reported to the RESC will be reported to ES-ISAC.
- D. Maintain Documentation.** The area or facility manager is responsible for maintaining relative documentation related to potential reportable incidents, incident response plan annual tests, and incident response plan annual review for the previous calendar year. The Director, IRO shall maintain records of all events received via the RESC, documentation supporting the decision to report or not to report to the ES-ISAC, and any related follow-up activities. All documentation records associated with incidents reported to ES-ISAC shall be maintained by the area or facility manager and the Director, IRO for 3 calendar years.
- E. Recovery Planning.** The area or facility manager must develop recovery plans specific to the local CCA. These plans must be reviewed on an annual basis and must address the following at a minimum:
- (1) roles and responsibilities must be determined for recovery team participants;
 - (2) methods must be developed to communicate responsibilities to all recovery participants;
 - (3) identification of potential failures, development of activation criteria, and procedures for recovery of the CCA;

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (4) procedures for performing backup and storage of information and other preparations as appropriate to execute recovery plans; and
- (5) procedures for testing backup storage and testing of recovery plans.

F. **Recovery Plan Exercises, Execution, and Revisions.** The area or facility manager must exercise the recovery plans annually. An exercise of the recovery plan can range from a paper drill, to a full operational exercise, to recovery from an actual incident. Backup media, essential to CCA recovery, shall be tested at least annually to ensure media is functioning properly. When a failure occurs, recovery plans must be initiated as soon as the failure analysis is properly recorded and any evidence associated with sabotage is properly documented. The recovery plan must be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan within thirty calendar days of the change being completed.

- 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.