

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Identification and Protection of Critical Cyber Asset (CCA) Information Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish a single, Bureau of Reclamation-wide process to identify and protect information associated with CCAs to promote the protection and 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); Computer Security Act of 1987 (January 8, 1988; Pub. L. 100-235); 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); Executive Order (EO) 12958, as amended; EO 12968; Office of Management and Budget Circular A-130, Appendix III.
- Approving Official:** Director, Information Resources Office (IRO)
- Contact:** IRO, 84-21000
Security, Safety, and Law Enforcement (SSLE), 84-45000

1. **Introduction.** The NERC Reliability Standards establish requirements addressing the identification and protection of information related to CCAs to better support the defense of cyber-controlled and monitored BES assets from cyber-based security threats, vulnerabilities, and incidents. Reclamation's existing Reclamation Manual (RM) D&S, *Identifying and Safeguarding For Official Use Only (FOUO) Information* (SLE 02-01) addresses protection requirements for sensitive information. This D&S provides additional requirements related to information associated with CCAs as defined in the Reliability Standards and must be used in conjunction with the above referenced RM component.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

2. **Applicability.** This D&S is applicable to all Reclamation offices, employees, contractors, consultants, and others. The requirements of this D&S must be applied to all FOUO information associated with CCAs as defined in this D&S.
3. **Definitions.**
 - A. **Authorized Access Individuals List.** A list of individuals authorized to grant access to FOUO information associated with CCAs. Personnel must be identified by name, title, and the information for which they are authorized to grant access.
 - B. **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.
 - C. **Critical Asset (CA).** A facility, system, or equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.
 - D. **CCA.** A cyber asset, including programmable electronic devices, communication networks, hardware, software, and data that is essential to the reliable operation of one or more CAs.
 - E. **Directors.** Reclamation Senior Executives responsible for specific programs or facilities. This definition includes, but is not limited to: the Director, Technical Resources; regional directors; Director, SSLE; Director, Policy and Administration; and Director, IRO.
 - F. **Electronic Security Perimeter (ESP).** An ESP is 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 requirements of this D&S, its companion D&S, and overarching policy.
 - G. **Information.** Facts, data, and knowledge created, received, and maintained for use by Reclamation to document its program decisions and mission-related activities, regardless of storage media, format, and nature or location of storage (including information maintained in centralized data repositories).
 - H. **Reliability Standards.** Any of a number of NERC or Western Electricity Coordinating Council 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

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

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 development of an information protection program to protect FOUO information, including access control requirements.
- C. **Directors.** Directors, or their delegates, are responsible for implementing the information protection program in their regions. This includes, ensuring that FOUO information associated with CCAs is properly identified, categorized, marked, and protected. Directors shall implement and maintain a list of authorized access approval individuals who are authorized to grant access to FOUO information associated with CCAs. Directors shall conduct an annual assessment of the information protection program(s) in their offices.
- D. **Authorized Access Approval Individuals.** Individuals authorized to approve access to FOUO information associated with CCAs are responsible for determining, based on their situational awareness and best judgment, that a prospective recipient requires access to specific FOUO information associated with CCAs in order to perform or assist in a lawful and authorized governmental function that is beneficial to Reclamation.

5. **Procedures.**

- A. **Identification of FOUO Information Associated with CCAs.** The information listed below shall be identified and safeguarded as FOUO information.
 - (1) the list of CAs developed in support of CIP-002;
 - (2) the CCA list developed in support of CIP-002;
 - (3) all non-public information relating to the operation of the specific cyber asset identified on the CCA list;

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (4) all drawings or documents, including floor plans or equipment layouts, which identify the physical location of the specific cyber asset identified on the CCA list;
 - (5) any network diagram which includes the specific cyber asset identified on the CCA list;
 - (6) any document which defines the ESP associated with the specific cyber asset identified on the CCA list;
 - (7) any document which defines the Physical Security Perimeter associated with the specific cyber asset identified on the CCA list;
 - (8) any security assessment of electronic or physical access to the specific cyber asset identified on the CCA list;
 - (9) any incident response plan which identifies the performance or security of the specific cyber asset identified on the CCA list; and
 - (10) any disaster recovery plan which contains the information related to the physical access, performance, or security of the specific cyber asset identified on the CCA list.
- B. Categorization, Marking, and Protection of FOUO Information Associated with CCAs.** All FOUO information associated with CCAs identified for protection in this D&S will be categorized, marked, and protected as FOUO information, in accordance with SLE 02-01.
- C. Access to FOUO Information Associated with CCAs.** Permission to access FOUO information associated with CCAs shall be granted on the basis of “need to know” by an individual on the authorized access approval list.
- 6. Authorized Access Individual List.** Lists of authorized access individuals must be developed and maintained as part of the overarching information protection program. Lists shall be updated at any time there is a change of roles, but must be formally reviewed and verified annually. Lists shall be maintained for a period of not less than 1 calendar year after any changes.
- 7. Annual Assessment.** Directors will annually review their adherence to the identification, categorization, and safeguarding requirements outlined in this D&S. Reviews and any necessary corrective actions will be documented and maintained for audit purposes.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

8. **Unauthorized Access.** Where unauthorized access to FOUO information associated with CCAs is detected, it shall be treated as an incident and reported per requirements outlined in the Temporary Reclamation Manual Release (TRMR) D&S, *Cyber Security Incident Response and Recovery Program Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-44).
9. **Related D&S.** Related and supporting D&S, as well as overarching Policy, are available in the Information Resources Management (IRM) and Security, Safety, and Law Enforcement (SLE) sections of the Reclamation Manual.