

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Cyber Asset Access Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish consistent, Bureau of Reclamation-wide requirements and criteria for the control and monitoring of physical and logical access to Critical Cyber Assets (CCA), associated CCA protection systems, and CCA information in support of the protection and reliability of the bulk electric system (BES). The benefit of this Directive and Standard (D&S) is that it promotes compliance with the Critical Infrastructure Protection (CIP) Reliability Standards of NERC.
- Authority:** Computer Security Act of 1987 (January 8, 1988; Pub. L. 100-235); Floyd D. Spencer 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); Federal Energy Regulatory Commission approved NERC Reliability Standards (18 CFR Part 40); Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (December 24, 1985; 50 Federal Register 52730); OMB Circular No. A-123, *Management Accountability and Control* (June 21, 1995; 31 U.S.C. § 3512); *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
Security, Safety, and Law Enforcement (SSLE), 84-45000

1. **Introduction.** The NERC CIP Reliability Standards establish logical and physical requirements designed to defend cyber-controlled and monitored BES assets from cyber-based security threats, vulnerabilities, and incidents. The protection requirements are applicable to essential cyber systems and cyber assets based on the identification of these assets as CCA supporting Critical Assets (CA) that are elements of the BES. This Directive and Standard (D&S) establishes requirements and criteria to support the management of access to physical spaces, and cyber systems.
2. **Applicability.** This D&S applies to Directors, supervisors, and all staff responsible for controlling physical and logical access to cyber systems, cyber subsystems, and cyber-based assets directly supporting Reclamation's facilities identified as CA.

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. **CA.** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.
- C. **CCA.** Cyber Assets essential to the reliable operation of CA. This specifically includes computers, computer network components, and cyber-based peripheral and protective systems that are essential to the reliable operation of the BES.
- D. **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.
- E. **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 access control requirements of this D&S, its companion D&S, and overarching policy.
- F. **Incident.** An incident is a security alert known to constitute a violation of law or policy – or an alert that has led to the jeopardizing of infrastructure, facilities, personnel, or information.
- G. **Incident Response.** The preparation, detection, and analysis of an incident.
- H. **Physical Access Control System (PACS).** A PACS is a cyber-based system that supports the protection, access control, and access monitoring of a Physical Security Perimeters (PSPs). PACS may also be referred to as Electronic Access Control and Surveillance Systems.
- I. **Physical Access List.** A list of personnel that have been granted unescorted physical access to a PSP.
- J. **Logical Access List.** A list of personnel that have been granted logical access to a CCA.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- K. **PSP.** A PSP is a physical, completely enclosed (“six wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which cyber assets are networked within an ESP and housed and for which physical access is controlled.
- L. **Recovery.** Recovery will include all efforts to contain and remove a problem associated with the cyber asset system functionality. The recovery also includes the process of restoring failed components to their original functioning status prior to the incident.
- M. **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 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.
- N. **Security Alerts.** Security alerts occur as a result of security status monitoring of logical ESP access and logical access to cyber assets within the ESP. Security alerts are issued by continuous monitoring functions and may include asset failure or unauthorized access, usage, configuration changes, network traffic, code execution, or login attempts.
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.
- B. **Director, SSLE.** The Director, SSLE is responsible for all criminal investigations performed for incidents at Reclamation’s facilities.
- C. **Technical Resources, Senior Advisor, Hydropower.** The Senior Advisor, Hydropower administers the Electric Reliability Compliance Program.
- D. **Directors.** The Directors are responsible for the security of CA and CCA within their directorate. The Directors are responsible for ensuring completion of documentation identifying personnel with logical access or unescorted physical access to CCA.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- E. **Reliability Compliance Representative.** As described 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.
- F. **Area and Facility Managers.** Area and facility managers are responsible for authorizing logical or physical access to CCA, and are accountable for performing and documenting activities within their respective area or facility office(s) to become and maintain compliance with this D&S, including the documentation of re-delegation of access authorization responsibilities. The area and facility managers shall be responsible for providing notification or developing a notification process so any changes in personnel logical or physical access rights are implemented within the time requirements dictated in this D&S.

5. Procedures.

A. Physical Access to Critical Cyber Assets.

- (1) **Identification of Access Points.** All physical access points and measures (i.e., card key, special locks, security personnel, biometric, keypad, token or equivalent device) to control entry to the PSP shall be identified and documented in a Physical Security Plan as outlined in the Reclamation Manual release concerning Physical Security Plans.
- (2) **Qualifications for Access.** Unescorted physical access into the PSP shall be supported by:
 - (a) documentation of an operational need for physical access;
 - (b) completion of an assessment of personal risk as outlined in Reclamation Manual Temporary Reclamation Manual Releases (TRMR) D&S, *Personnel Risk Assessment (PRA) Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance (IRM TRMR-39)*;
 - (c) completion of the local authorized access form included in the facility specific Physical Security Plan; and
 - (d) completion of training as outlined in Reclamation Manual TRMR D&S, *Security Awareness and Cyber Security Training Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance (IRM TRMR-38)*.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (3) **Physical Access List.** The area or facility manager may grant an individual unescorted physical access, once all the requirements in Paragraph 5.A.(2) have been completed. Granting of access, including specific physical access rights (by named PSP), must be documented in a Physical Access List.
- (4) **Maintenance of Physical Access List.** The Physical Access List shall be maintained for each facility. The list shall be updated within 7 calendar days of any change. The list shall be reviewed quarterly.
- (5) **Monitoring of Physical Access.** Procedural and technical controls shall be implemented and documented for monitoring physical access at all access points into the PSP. Physical access monitoring methods provided by alarm systems or by human observations shall be implemented to identify unauthorized access attempts. Any identified unauthorized access or access attempts shall be reviewed immediately and handled as outlined in the Reclamation Manual release concerning cyber security incident response and recovery supporting NERC reliability standard compliance.
- (6) **Logging of Physical Access.**
 - (a) Logging of physical access shall be implemented 24 hours a day, 7 days a week. Logs of the monitored data must be produced and retained for a minimum of 90 days. Logging mechanisms shall record sufficient information to uniquely identify individuals, time of entry, and date. One or more of the following logging methods must be implemented:
 - (i) electronic access control system logs;
 - (ii) video recording; and/or
 - (iii) or manual logging
 - (b) Any unauthorized access or unauthorized access attempts reflected within the logs shall be investigated and handled as outlined in Reclamation Manual D&S concerning cyber security incident response and recovery supporting NERC reliability standard compliance.
- (7) **Protection of PACS Cyber Assets.** All cyber assets that are components of a PACS associated with the protection of an identified ESP shall be protected from unauthorized access. Those cyber assets must be provided with the security

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

controls required to meet the NERC CIP requirements for protection of a PACS (see NERC CIP-006 R2.2, the protections are identified in CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R4 and R5, CIP-007, CIP-008, and CIP-009).

- (8) **Protection of Cyber Assets Controlling Access to an ESP.** All cyber assets that are components of an access control system that provides access control and/or monitoring of an ESP must reside in an identified PSP. Further, those cyber assets must be provided with the security controls required to meet the NERC CIP requirements for protection of ESP access control systems (see NERC CIP-005 R1.5, the protections are identified in CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R3, CIP-007 R1 and R3-R9, CIP-008, and CIP-009).
- (9) **Maintenance and Testing of PACS Cyber Assets.** A program for periodic maintenance and testing of PACS must be implemented and documented. Testing must be performed no less frequently than every 3 years. Maintenance of the PACS must be documented and performed as required in the program documentation.
- (10) **Records Retention.** Outage records for PACS (including an outage of any portion of the system that protects an ESP) must be retained for a minimum of 1 year. Testing and maintenance records for PACS, test procedures, or test processes must be retained for a minimum of one testing or maintenance cycle.
- (11) **Reviews of Physical Access.** A review of those individuals that have been granted unescorted physical access (see the physical access list) shall be conducted quarterly by facility or area managers to determine if access rights are appropriate. Documentation shall indicate who conducted the review, when the review took place, and the changes that were made.
- (12) **Changes / Revocations of Physical Access.** Any revocations of physical access rights for cause must be accomplished within 24 hours of the change. Revocations of physical access shall be supported by procedural controls to ensure protection of critical cyber assets. Other changes or revocations of physical access rights must be accomplished and documented within 7 calendar days.

B. Logical Access to Cyber Assets from within the ESP.

- (1) **User Level Access Protection.** Each cyber asset within the ESP that is accessible must be configured for secure logical access or secure user level access. Logical access can include an operator who requires access to a console or a programmer that requires access to a particular software element for maintenance purposes.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

Logical access to all cyber assets within the ESP must be protected by documented technical and procedural controls that enforce access authentication. Logical access includes but is not be limited to the following:

- (a) individual or shared accounts (see additional information concerning shared accounts in Paragraph 5.B.(5) below) for network devices such as firewalls, routers, and switches;
 - (b) administrative or user accounts for intrusion detection and network monitoring systems;
 - (c) accounts used for configuration of PLCs or other network enabled plant devices; and
 - (d) user and operational accounts for cyber systems such as SCADA (Supervisory Control and Data Acquisition) or access control for cyber assets within an ESP.
- (2) **Qualifications for Access.** Any electronic access (user accounts) must meet all of the following conditions prior to the creation of the account or access to the account:
- (a) access authorizations and permissions that are consistent with the concept of “need-to-know” with respect to work functions performed;
 - (b) the completion of an assessment of personal risk as outlined in Reclamation Manual D&S, *Personnel Risk Assessment (PRA) Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-39);
 - (c) the completion of training as outlined in Reclamation Manual D&S, *Security Awareness and Cyber Security Training Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-38); and
 - (d) be provided any local training for routine or emergency operations and other system specific requirements outlined in a “rules of behavior” or similar appropriate use documents as deemed necessary by the area of facility manager.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (3) **Logical Access List.** The area or facility manager may grant an individual logical access to CCA once all the requirements in Paragraph 5.B.(2) have been completed and must maintain a list of users. Automated mechanisms developed to identify authorized logical users, (e.g., active directory user lists) will also satisfy this requirement.
- (4) **Maintenance of Logical Access List.** The Logical Access List for each facility shall be maintained. The lists shall be updated within 7 calendar days of any change and be reviewed quarterly.
- (5) **Shared Account Usage.** For Reclamation cyber assets, usage of shared accounts, such as administrator accounts, factory provided default accounts, and other accounts that are not assigned to a unique user, shall be minimized and managed in scope and acceptable use. Only those personnel identified and approved will be provided shared account access. Passwords for shared accounts must be changed when an individual no longer requires usage of the account.
- (6) **Passwords.** At a minimum, cyber assets must enforce passwords that meet the following requirements or technical feasibility exceptions (TFE) must be obtained:
 - (a) Each password shall be a minimum of six characters.
 - (b) Each password shall consist of a combination of alpha, numeric, and special characters.
 - (c) Each password shall be changed at least annually.
- (7) **Logging of Electronic Access.** Procedural and technical controls shall be implemented and documented for electronic logging for all cyber assets within the ESP. Logs for user activity must uniquely identify the user gaining access, or account name for shared accounts, the type of access (user/administrator), and the access activity period. Access activity logging must capture information at both the operating system level (applications started/stopped) and, where practical, the application level. Details captured must allow a qualified reviewer to identify cyber activities that fall outside the user's responsibilities, roles, or authorities. These logs must be maintained for no less than 90 days.
- (8) **Monitoring of Electronic Access.** Procedural and technical controls shall be implemented and documented for electronic monitoring of all cyber assets within the ESP. Electronic monitoring shall be implemented 24 hours a day, 7 days a week. The monitoring process shall detect and provide system security alerts that

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

must be reviewed at least weekly. Where the electronic monitoring or alert capability is not technically feasible, compensating measures shall be implemented and documented accordingly and associated TFEs shall be submitted. When the automated alerts are not possible, manual review of electronic logs for security alerts must be performed at least every 90 days. Logs related to reportable incidents shall be maintained for 3 years as outlined in the Reclamation Manual release concerning cyber security incident response and recovery supporting NERC reliability standard compliance.

- (9) **Reviews of Electronic Access.** A review of those individuals who have access shall be conducted and documented quarterly to determine if access rights are consistent with the organizational authorizations and are still required. Documentation shall indicate who conducted the reviews, when the review took place, and any necessary changes.
- (10) **Changes/Revocations of Electronic Access.** Changes to access rights related to revocations for cause shall be accomplished within 24 hours. Any change to user access rights shall be revised and accomplished accordingly within 7 days, including normal revocations. For cyber assets where revocation of physical access prevents all logical access, it will be acceptable to revoke only physical access to the assets within the 24-hour timeframe. All user access rights must be revoked within 7 days.

C. Logical Access into an ESP.

(1) Electronic Access.

- (a) Electronic access into the ESP includes:
 - (i) external or remote access into the electronic access points;
 - (ii) dial-up access to a cyber asset within the ESP; and
 - (iii) third party data link or vendor account interconnections.
- (b) Electronic access into the ESPs must be protected by organizational processes, procedures, and technical mechanisms as outlined in the Reclamation Manual release concerning electronic security perimeters identification supporting NERC reliability standard compliance.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (2) **Third Party Interconnections.** Third party interconnections include all data interconnections from other government agencies, private companies, vendors, or contactors that originate from cyber systems or equipment that are not under the direct supervision of Reclamation's directors and communicate through an ESP access point to Reclamation cyber assets. The following processes and procedures shall be implemented:
- (a) **Agreements.** Directors are responsible for the authorization of interconnection agreements to support the control of electronic access for third party interconnections. The responsibility may be passed on to local staff provided it is identified and documented accordingly (this is not a formal delegation of authority). Interconnection agreements shall be maintained by the Directors. Agreements shall be reviewed, revised, or revoked as appropriate. Implementation of and any changes to agreements shall be reported to the IRO within no more than 60 days of the change.
 - (b) **Interconnection Security Agreements.** Maintenance/support contract language, interconnection security agreements (ISAs) or Memorandums of Understanding (MOUs) shall be documented and signed by all parties representing interconnections into Reclamation ESPs. The agreements must document the type of connectivity, required ports, access controls, electronic protection mechanisms, logging, and user account authentication.
 - (c) **Vendor Support Accounts.** Contract language, ISAs or MOUs supporting remote vendor access shall document the required authorizations of user accounts, access control procedures and mechanisms, and logging. Vendor user accounts will be established only for individual users in accordance with B(2) above. Vendor accounts will only be established for the time period they are required, and they must be removed or disabled when not in use.
- (3) **Remote Interactive Access (Account Access).** When remote access is required for interactive use of an account on a cyber asset within an ESP, all of the requirements associated with the section above, *Logical Access to Cyber Assets within the ESP* (Section 5.B), will apply.
- (4) **Monitoring and Logging of Electronic Access.** The monitoring and logging requirements for electronic access into the ESP are the same as to those requirements found in Paragraph 5.B.(7) and (8). Monitoring of dial-up access into the ESP must be performed where possible. Automated security alerts shall be provided 24 hours a day/7 days a week and reviewed at least weekly. When the automated alerts are not possible and manual review of logs is necessary to detect unauthorized access, those access logs shall be reviewed at least every 90 days.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (5) **Appropriate Use Banner.** Devices that allow interactive access into an ESP shall display an appropriate use banner on the user screen when access is attempted. The Director, IRO will maintain a narrative of a full banner that shall be used for cyber assets that allow ESP interactive access; however, a condensed version will also be provided for situations where the full banner cannot be displayed. When neither of the banners can be displayed, the full banner must be posted in a location directly visible and legible by a user accessing the device.
- D. **Emergency Access.** Physical access may be permitted to CCA by qualified and recognized emergency responders and law enforcement officials who have not successfully completed required training in times of emergency. Such access will be granted by an authorized Reclamation official and shall extend to the duration of the emergency unless otherwise noted. Any access afforded in this manner must be officially documented in access logs with a notation for the cause.
6. **Related D&S.** Related and supporting D&S, as well as overarching Policy, are available in the Information Resources Management (IRM) and Security and Law Enforcement (SLE) sections of the Reclamation Manual. See Reclamation Manual D&S, *Critical Cyber Asset (CCA) Identification supporting North American Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-34) for additional information.