

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Configuration Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish specific requirements for a single, Bureau of Reclamation-wide process for configuration management of cyber assets subject to the NERC Critical Infrastructure Protection (CIP) Reliability Standards 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 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); 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.** This D&S details the configuration management requirements for cyber assets that are subject to the NERC CIP Reliability Standards. Reclamation's configuration management process, as defined below, incorporates various requirements including, creation of a methodology for establishing a configuration baseline, approval of changes to the configuration baseline, and tracking of approved changes to the configuration baseline.
2. **Applicability.** This D&S applies to all directors, supervisors, and staff responsible for configuration management of cyber assets as defined by the NERC CIP Reliability Standards that support Reclamation power and attendant facilities operated and maintained directly by Reclamation staff.

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).** A facility, system, or equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.
- C. **Critical Cyber Asset (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. **Directorate.** The organizational component of a Director. This includes the Director, Technical Resources; regional directors; Director, Security, Safety, and Law Enforcement (SSLE); Director, Policy and Administration; and Director, IRO.
- E. **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.
- F. **Configuration Control.** The process of controlling modifications to a system's design, hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation.
- G. **Configuration Control Board (CCB).** An established committee that is the final authority on all proposed changes to systems or applications.
- H. **Configuration Identification.** The baseline configuration for the security controls associated with the CCA and other cyber assets. The baseline configuration includes, at a minimum, available ports and services, account access controls, additional security hardening, installed anti-virus/malware software, and settings for intrusion detection software.
- I. **Configuration Item.** The smallest component of hardware, software, firmware, documentation, or any of its discrete portions, which is tracked by configuration management. These items also include components of networks or communications systems.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- J. **Configuration Management.** The management of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the life cycle of the system.
- K. **Configuration Management Plan (CMP).** A document describing how configuration management will be implemented to achieve the four basic goals of identification, control, accounting, and auditing. It identifies the configuration items, roles, and responsibilities.
- L. **Electronic Security Perimeter (ESP).** An ESP is the logical border surrounding a network to which CCA are connected and for which access is controlled.
- M. **Physical Security Perimeter (PSP).** A PSP is a physical, completely enclosed (“six wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which CCA are housed and for which access is controlled.
- N. **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).
- O. **Reliability Standards.** Any of a number of NERC or Western Electricity Coordinating Council (WECC) Standards, the specific requirements of which are applicable to Reclamation, 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.
- P. **“Significant” Changes.** Significant changes are defined as changes that affect the functionality or security controls of the cyber assets subject to the NERC CIP Reliability Standards. Significant changes are defined by NERC as security patches, operating system upgrades/service packs, revisions to applications, and changes to third-party software or firmware. Significant changes would also include the removal or replacement of cyber assets or any other asset identified as a “configuration item.”
- Q. **Technical Feasibility Exception (TFE).** An exception from strict compliance with the terms of an applicable NERC CIP requirement on the grounds of technical feasibility or technical limitation. For more information see *NERC Compliance Process Bulletin No. 2009-007*.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

4. Responsibilities.

- A. **Area Managers or Facility Managers.** Area managers or facility managers are responsible for performing and documenting activities within the area or facilities office to maintain or become compliant with all NERC CIP Reliability Standards.
- B. **Director, IRO.** The IRO has overall responsibility for configuration management of information technology (IT) systems in Reclamation. In addition, the 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.
- C. **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.
- D. **Configuration Control Board (CCB).** Regional directors shall establish CCBs to review, evaluate, and approve (or disapprove) proposed changes to cyber assets subject to the NERC CIP Reliability Standards. In general, it is recommended that a CCB be established to oversee configuration management for cyber assets at a particular CA facility, control center, or area office; however, when appropriate, a CCB must oversee multiple facilities or control centers as required.
- E. **Regional Directors.** Regional directors or their delegate are responsible for the execution and documentation of all applicable NERC compliance activities within the region to maintain or become compliant with all NERC CIP Reliability Standards, including the support and coordination of IT related compliance requirements with the IRO. Regional directors are responsible and accountable for ensuring that configuration management requirements are met for CCAs or other cyber assets subject to the NERC CIP Reliability Standards including establishing CCBs to manage the changes to all components. All such activities shall be focused on achieving, maintaining, and supporting demonstrable evidence of compliance with the NERC CIP Reliability Standards.
- F. **Information System Security Manager (ISSM).** ISSMs are the principal technical advisors to the regional director for all security-related issues. ISSM generally manage and oversee configuration management practices on behalf of the regional director.
- G. **IT Technical Teams.** For those systems which include platforms supported by Reclamation IT Technical Teams, these teams are responsible to provide consulting,

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

coordination, standards, procedures, and testing. IT Technical Teams will recommend changes to the CCB, act as liaison to the CCB, and coordinate with IT technical staff to ensure effective implementation of configuration management practices.

- H. **Reliability Compliance Representative.** Unless otherwise indicated and documented by the directorate, the reliability compliance representative is responsible for coordinating directorate compliance-related activities and reporting compliance status for the directorate.
 - I. **Information System Security Officer (ISSO).** ISSOs participate in the configuration management process to ensure that security is not degraded, but only enhanced (or maintained at the same level) as a result of changes. The Reclamation ISSOs coordinate with system administrators to ensure effective implementation of configuration management practices.
5. **Procedures.** The configuration management program for a particular CA must include the establishment of local procedures to accomplish the following:
- A. **CCB.** For all cyber assets that are subject to the NERC CIP Reliability Standards, a CCB must implement configuration management in support for adding, modifying, replacing, or removing hardware or software. These activities must identify, control, and document all entity or vendor related changes to hardware and software components for cyber assets subject to the NERC CIP Reliability Standards pursuant to a CMP.
 - (1) **Membership.** At a minimum, the CCB shall include a CCB chairperson and a group of knowledgeable professionals who will review, evaluate, and approve (or disapprove) changes. As circumstances require, depending on the nature of changes being considered, the CCB membership may include other key individuals from physical security, facilities, quality assurance, budget, etc.
 - (2) **Activities.** The CCB will meet on an as-required basis to approve or disapprove changes; members will communicate with each other regularly by e-mail, telephone, and similar means during the review and evaluation process. Any formal documents, such as meeting minutes, that represent the approval or disapproval of the proposed changes must be maintained for at least 2 years.
 - B. **CMP.** All CCAs or other cyber assets subject to the NERC CIP Reliability Standards must be included within a CMP. A single CMP can address multiple systems or applications and must identify all applicable cyber assets or refer to other documents to identify assets placed under configuration management. The CMP will describe how configuration management is being (or will be) accomplished, and it will identify the

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

configuration items for each system or application. The CMP will be approved and signed by the chairperson of the CCB. At a minimum, the CMP must include the following items:

- (1) list CCB participants by title or position;
- (2) roles and responsibilities of CCB members;
- (3) configuration identification - system or application description, boundaries, documentation references, a list of configuration settings, and a list of security control settings including any tools available to assist in the configuration management process;
- (4) configuration control - normal procedures for configuration control including classification of change requests, assessment of change risk, planning requirements, development methods, peer reviews, off-line testing, and on-line testing (note impacts on related systems and how they will be addressed); and
- (5) configuration accounting and documentation procedures.

C. **Configuration Identification.** The configuration baseline for cyber assets subject to the NERC CIP Reliability Standards must be identified for the purpose of systematically controlling changes to maintain the integrity and traceability of any change throughout the system life cycle. References to other documents are appropriate support for configuration identification. First, the scope and boundaries of the system must be identified. Second, the security controls for the system must be identified.

- (1) **System Scope.** All cyber assets subject to the NERC CIP Reliability Standards must be inventoried and documented. Requirements for the identification of these cyber assets are addressed in Reclamation Manual Temporary Reclamation Manual Release (TRMR) D&S, *Critical Cyber Asset (CCA) Identification Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-34).
- (2) **Security Control Identification.** Hardware and software associated with cyber assets subject to the NERC CIP Reliability Standards must be identified and documented, including the minimal ports and services required for normal and emergency operations. The configuration baseline must also identify the security patches, malicious software prevention software and settings, account configurations, and any additional configuration settings. For additional information on the configuration of ports and services refer to *Appendix A, Ports and Impact Analysis Testing*, and for account configurations refer to Reclamation

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

Manual TRMR D&S, *Cyber Asset Access Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-42).

- D. **Configuration Control.** Procedures must address systematic testing, evaluation, coordination, and approval or disapproval of proposed “significant” changes to the design and construction of any cyber assets subject to the NERC CIP Reliability Standards. The CMP must define what changes will be addressed and provide requirements as to how the changes will be implemented and how the security controls on the impacted devices will be validated to ensure they have not been adversely affected.
- (1) **Testing Procedures.** Test procedures are required to ensure that any “significant” change has not adversely affected existing cyber security controls. Test procedures must be executed for any new cyber assets subject to the NERC CIP Reliability Standards and existing impacted applicable cyber assets. All testing must be accompanied with an effort to minimize any adverse effects on the production system. Separate “test” systems and environments must be utilized for such testing provided that the “test” system, in instances where such testing cannot be performed on an operational system, is utilized with testing performed in a manner that reflects the production environment.
 - (2) **Security Patch Management.** A program must be established for the tracking, evaluating, testing, and installing of applicable cyber security software patches for all cyber assets subject to the NERC CIP Reliability Standards. To determine applicability, all security patches and security upgrades must be assessed within 30 calendar days of the availability of the patch or upgrade. Vendor provided documentation indicating applicability of a proposed patch can be used to satisfy the assessment requirement. Where an applicable patch or upgrade cannot be installed, the supporting justification and the identification of compensating measures applied to mitigate the risk must be documented.
 - (3) **Anti-virus and Malware.** Anti-virus and malware software must be utilized to detect, prevent, and mitigate the introduction, exposure, and propagation of all malware on cyber assets subject to the NERC CIP Reliability Standards. The implementation of all anti-virus and malware prevention tools must be documented including the process and procedures related to “signature” update and testing. Individual periodic updates of anti-virus and malware prevention software “signatures” will not need to be addressed by the CCB; however, the methods that are followed to accomplish the “signature” updates, including how those updates are tested prior to deployment, must abide by configuration control procedures that have been authorized by the CCB.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (4) **Disposal and Redeployment.** Formal methods, processes, and procedures must be documented and implemented for the disposal or redeployment of CCA and other cyber assets subject to the NERC CIP Reliability Standards. When CCA or other cyber assets subject to the NERC CIP Reliability Standards are replaced, taken out of service, or redeployed, those assets and associated documentation must be managed within the configuration management process. Changes or deletions to the CCA inventory must be maintained as dictated within the CMP. Records of the disposal and/or redeployment must be documented and maintained pursuant to Reclamation Manual D&S, *Reclamation Information Technology (IT) Security Program (ITSP): IT Asset Disposal – Information Sanitization* (IRM 08-13).
- E. **Configuration Status Accounting.** The goal of configuration status accounting is to record and report all information considered “significant” to the configuration management process. The documentation produced and revised through configuration management process must be reviewed as dictated by the CMP. For additional information on the documentation that must be managed within the CMP see, *Appendix B, Configuration Management Documentation*. All documentation associated with cyber asset testing, ports and services, patch management, malicious code, account management, security status monitoring, asset disposal or redeployment must be reviewed annually and revised within 30 calendar days of performing a significant change to any CCA or other cyber assets subject to the NERC CIP standards asset. Documentation associated with a change to an ESP must be revised in 90 calendar days. For more information, refer to Reclamation Manual TRMR D&S, *Electronic Security Perimeter (ESP) Identification Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-45).
6. **Related D&S.** Related and supporting D&S, as well as the overarching Policy, are available in the IRM section of the Reclamation Manual. For more information on Reclamation CA see Reclamation Manual TRMR D&S, *Critical Asset (CA) Identification Supporting NERC Reliability Standard Compliance* (IRM TRMR-35).