

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- Subject:** Personnel Risk Assessment (PRA) Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
- Purpose:** To establish specific requirements for a single, Bureau of Reclamation-wide process for risk assessment of personnel with access to Reclamation Critical Cyber Assets (CCAs) 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 improved compliance with the Critical Infrastructure Protection (CIP) Reliability Standards of NERC.
- Authority:** The Reclamation Act of 1902 (Act of June 17, 1902, ch. 1093; 32 Stat. 388), the Town Sites and Power Development Act of 1906 (Act of April 16, 1906, ch. 1361, 34 Stat. 116), Federal Power Act of 1920 (Act of June 10, 1920, ch. 285, 41 Stat. 1063), Reclamation Project Act of 1939 (Act of August 4, 1939, ch. 418, 53 Stat. 1187), Department of Energy Act of 1977 (Act of August 4, 1977, Pub. L. 95-91; 91 Stat. 565), Energy Policy Act of 1992 (Act of October 24, 1992, 106 Stat. 2776), Energy Policy Act of 2005 (Act of August 8, 2005, 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
Security, Safety, and Law Enforcement (SSLE), 84-45000
Policy and Administration, Human Resources Division, 84-58000
-

1. **Introduction.** The NERC CIP Standards establish PRA requirements for individuals with unescorted physical and/or logical access to CCAs. Reclamation's PRA process is designed to provide a determination of the suitability of personnel with such unescorted physical and/or logical access. This D&S establishes requirements and criteria to support Reclamation's PRA activities.
2. **Applicability.** This D&S applies to all employees, contractors, vendors, operating partner personnel, temporary staff, and visitors who will be permitted logical or unescorted physical access to Reclamation's CCAs. This D&S is also applicable to supervisors and management responsible for the administration of the PRA process.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

3. **Definitions.** Definitions can be found in Appendix E.
4. **Responsibilities.**
 - A. **Director, Policy and Administration.** The Director, Policy and Administration is responsible for oversight of the PRA processes supporting identity verification and criminal check adjudication.
 - B. **Policy and Administration, Chief, Human Resources Division.** The Chief, Human Resources Division is responsible for the execution and documentation of processes to support the PRA. The respective human resource officer and the workforce relations officer (Denver and Washington offices) are responsible for furnishing summary adjudication information to the appropriate directorate office from which the request originated.
 - 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 Reliability Standards' compliance, as applicable, to NERC and the Western Electricity Coordinating Council (WECC).
 - D. **Director, IRO.** The Director, IRO, is identified as Reclamation's senior manager with overall responsibility for leading and managing the implementation and adherence to the NERC CIP Standards, CIP-002 through CIP-009.
 - E. **Director, SSLE.** The Director, SSLE, is responsible for the establishment of compliance measures supporting PRAs for Reclamation personnel, contractors, vendors, and visitors with unescorted physical or logical access to CCAs.
 - F. **Directors.** Each director is responsible for the establishment, execution, and documentation of all compliance activities related to PRA within their directorate. This includes the appropriate control of access and the collection, coordination, and submittal of information as necessary to support the completion of PRAs on their personnel, contractors, vendors, and visitors requiring access to CCAs over which the directorate has oversight.
 - G. **Reliability Compliance Representative.** Unless otherwise indicated and documented by the directorate, the Reliability Compliance Representative is responsible for coordinating directorate PRA needs, procedures, information submittals, and completions as necessary to support needed access to CCAs.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- H. **Area and Facility Managers.** Area and facility managers responsible for identified CCAs are also responsible and accountable for ensuring that PRAs are performed (or re-performed, as necessary) and documented on all individuals with access to those CCAs in order to comply and maintain compliance with this D&S.
- I. **Background Investigation Adjudication Offices.** Reclamation's background investigation adjudication offices (i.e., human resources and security offices) that are presently responsible for completing and adjudicating background investigations on Federal employees are hereby identified as responsible for performing and documenting PRAs on all individuals, including employees, contractors, vendors, operating partner personnel, temporary staff, and visitors that are subject to the requirements of this D&S.
5. **Procedures.**
- A. **PRA Process.** All Reclamation PRA efforts shall follow the process outlined in Appendix A and the related Appendices B, C, D, and E. Where practical, and as outlined in Appendix A, *Personnel Risk Assessment (PRA) Process*, Reclamation will leverage existing background investigation information (i.e., from Homeland Security Presidential Directive 12 and personal suitability processes) to support the PRA.
- B. **Periodic PRA Review.** All PRAs shall be reviewed no less frequently than every 7 years, subject to the requirements of Paragraph 5.C., below. Where practical, and in the interest of reducing costs, PRAs shall be conducted to enable them to support or coincide with other personnel background investigations.
- C. **Reassessments for Cause.** Notwithstanding the required 7-year periodic update of a PRA for any individual with unescorted physical or logical access to CCAs, Reclamation will conduct interim PRAs as necessary to assess potential risk related to an individual's access "for cause." In the event that a "for cause" PRA is not successfully completed for any reason, the individual must be denied unescorted physical or logical access to Reclamation's CCAs. "For cause" criteria include, but may not be limited to:
- (1) discovery of relevant and substantiated information regarding illegal activities, in accordance with Federal, state, or local statute; or
 - (2) other activities or conduct that would be reasonably interpreted to affect suitability for Federal employment or access to CCAs.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- D. **Protection of PRA Information.** Criminal background and identity verification information related to the PRA of individuals afforded unescorted physical or logical access to Reclamation CCAs is FOR OFFICIAL USE ONLY and is subject to protection under Reclamation Manual D&S, *Identifying and Safeguarding FOR OFFICIAL USE ONLY Information* (SLE-02-01).
- E. **Retention of PRA Records.** In accordance with NERC standards, information related to the risk assessment determination and results (adjudication results) for all individuals for whom a PRA has been conducted pursuant to access to CCAs shall be retained such that the risk assessment materials and determination results from the current (most recent) and previous PRA are always available for review or audit. See Appendix A for more information.
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. The D&S detailing access requirements can be found at IRM TRMR-42 *Cyber Asset Access Management Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance*.
7. **Appendices.**
- A. **Appendix A.** PRA Process.
 - B. **Appendix B.** Authorization for Release of Information.
 - C. **Appendix C.** Sample National Criminal History Check Determination Memorandum Template (Favorable Adjudication).
 - D. **Appendix D.** Sample National Criminal History Check Determination Memorandum Template (Unfavorable Adjudication).
 - E. **Appendix E.** Definitions.