Reclamation Manual

Policy

TEMPORARY RELEASE
(Expires 01/30/2025)

Subject: Operational Technology (OT) Remote Access Policy

Purpose: The purpose of this policy is to state the Bureau of Reclamation's decision regarding the use of remote access to Reclamation's OT assets and systems**.**

Authority: Privacy Act of 1974 (Pub. L. 93-579; 88 Stat. 1896; 5 USC 552a); Federal Managers' Financial Integrity Act of 1982 (Pub. L. 97-255; 31 USC 66a); Clinger-Cohen Act – Information Technology Management Reform Act of 1996 (Pub. L. 104-106); E-Government Act of 2002 (Pub. L. 107-347; 116 Stat. 2899; 44 USC 101); Federal Information Security Management Act (FISMA) of 2002, as amended (44 USC 3541); National Defense Authorization Act for Fiscal Year 2015 (January 3, 2014), Division A, Title VIII, Subtitle D-Federal Information Technology Acquisition Reform, Sections 831-837 (Pub. L. 113-291); Cybersecurity Information Sharing Act of 2015 (Pub. L. 114-113; 6 USC 1501); Office of Management and Budget (OMB) Circular A-130, Appendix III, *Cybersecurity of Federal Automated Information Systems*; OMB Circular A-123*, Internal Control Systems;* National Institute of Standards and Technology (NIST); Department of the Interior Departmental Manual Part 375 Chapter 19

Approving Official: Commissioner

Contact: Information Resources Office (IRO), Risk Management Services Division (RMSD), 84-21300

1. Introduction.

Reclamation relies on OT assets and systems that generate power, treat and deliver water, and monitor and protect facilities, to fulfill our mission, and cybersecurity threats against these types of systems are increasing. Failing to protect these systems from cyberattack could harm Reclamation infrastructure, disrupt services, threaten community safety, and prevent us from fulfilling our mission. To prevent a successful attack on these systems, Reclamation must ensure they are isolated from external networks.

2. Applicability.

This Policy applies to all Reclamation owned[1], operated, and/or maintained OT assets and systems, and all Reclamation employees[2] developing, installing, maintaining, and operating these OT assets and systems. Connections to Bonneville Power Administration and Western Area Power Administration are exempt from this policy due to operational necessity. One-way communications, outbound from the authorization boundary, through a RMSD approved unidirectional diode, are not considered remote access and thus, does not fall under the scope of this policy.

3. Policy.

Remote access to Reclamation OT is not allowed.

4. Deviation.

A. Requests.

Any deviation request for this policy must conform with requirements established in Reclamation Manual (RM) Directives and Standards, *Request for Deviation from a Reclamation Manual Requirement and Approval or Disapproval of the Request* (RCD 03-03).

(1) **Contents of the Deviation Request**. In addition to what is outlined in RCD 03-03, Paragraph 3.B., the following must be included:

(a) system name and acronym;

(b) system security categorization (if determined);

(c) system purpose;

(d) business justification for remote access;

(e) if the remote access is expected to be permanent or temporary;

[1] This includes systems owned by Reclamation but developed, installed, maintained or operated by a transferred works operator or contractor. If a system is owned by a transferred works operator, it does not fall under the scope of this Policy. However, unless there is complete certainty that an OT asset/system is owned by a transferred works operator, the assumption will be that it is Reclamation owned and be will subject to this Policy.

[2] When drafting acquisition requirements (i.e., a Solicitation's Statement of Work, Statement of Objectives, or technical specifications), the program/requesting office is responsible for including any OT requirements that are applicable to contract performance, deliverables, and/or contractor employees. The program/requesting office must also inform RMSD of applicable acquisition requirements relevant to this RM Policy.

(f) what users will be utilizing remote access (i.e., Reclamation employees, district employees, contractors, other federal agency employees, etc.),

(i) physical location of users, and

(ii) confirmation that users have a DOI Access PIV card or will only be granted access once they obtain a DOI Access PIV card;

(g) a description of type of work to be performed remotely;

(h) if the OT asset or system falls under North American Electric Reliability Corporation Critical Infrastructure Protection requirements; and

(i) assurance by the system owner that sufficient resources are available to implement and support the approved secure remote access solution.

(2) **Approval.** In addition to the requirements of RCD 03-03, approval will also be required by the Associate Chief Information Officer, who serves as the authorizing official (see Paragraph 4.J.(1) of RM *Delegations of Authority*), the only official with the authority to formally assume responsibility for operating information technology (IT)/OT systems at an acceptable level of risk.

B. Approved Remote Access Requirements.

If the deviation request is approved:

(1) The system owner must purchase and implement an RMSD approved secure remote access solution.

(2) The system owner must implement the additional security controls identified in the RMSD OT Remote Access Security Control Overlay.

5. Definitions.

A. Authorization Boundary.

All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

B. External Network.

Network that is not located within the system authorization boundary.

C. Operational Technology or OT.

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, to include Supervisory Control and Data Acquisition (SCADA) systems, and building management systems, fire control systems, and physical access control mechanisms.

D. Remote Access

Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network.

6. Review Period.

The originating office will review this release every 4 years.