Reclamation Manual

Policy

Subject: Information Management and Technology (IMT) Cybersecurity Program

Purpose: Defines and establishes the authorities and responsibilities for the Bureau of Reclamation's IMT Cybersecurity Program. The benefit of this Policy is to ensure compliance with all cybersecurity programs.

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.

This Policy establishes oversight, accountability, validation, and perspective for the appropriate management of risk to Reclamation's IMT resources. Risk management supports the achievement of strategic objectives; improvements in mission and operational capabilities; the delivery of services to internal and external customers; and addresses legislative requirements, policies, and directives issued by the Department and OMB.

2. Applicability.

This Policy applies to all Reclamation employees[1] using Reclamation-owned, -operated, or -maintained information technology (IT) assets and operational technology (OT) assets.

1 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 IRM P01 requirements that are applicable to contract performance, deliverables, and/or contractor employees.

3. Policy.

Reclamation's Associate Chief Information Officer (ACIO) will establish and administer an IMT Cybersecurity Program to comply with all relevant Federal requirements. These requirements are identified in annual Department Office of the Chief Information Officer (OCIO) memoranda, OMB circulars and memoranda, NIST publications, and Department and Reclamation policies and standards. These requirements are mandatory and govern the implementation, operation, and disposal of all IMT.

4. Program Oversight.

Reclamation employees with IMT program oversight authority and responsibility will ensure compliance with cybersecurity Federal laws, rules, regulations, policies, standards, and procedures.

A. The Commissioner will implement policies and procedures, as necessary, to ensure the ACIO has full visibility, accountability, and control over IMT.

B. The Deputy Commissioner, Policy, Administration and Budget will provide executive-level policy and program direction and guidance and maintain executive oversight of Reclamation's IMT Cybersecurity Program.

C. The ACIO will:

(1) oversee the development of Reclamation-wide cybersecurity policy, standards, and guidance by the Senior Advisor, OT/Industrial Control Systems (OT/ICS) Cybersecurity, RMSD,

(2) designate information system owners (ISO), and

(3) approve and/or deny all information system Authorization To Operate / Authorization To Use packages.

D. The Senior Advisor, OT/ICS Cybersecurity, manages Reclamation's IMT Cybersecurity Program.

E. The ISOs:

(1) have statutory, managerial, and operational authority for the information systems they are responsible for,

(2) will establish the procedures governing the implementation, operation, and disposal of information systems,

(3) designate information system security officers (ISSO), and

(4) provide cybersecurity requirements and controls for designated IMT.

F. Regional information system security managers (RISSM) are designated by regional directors to coordinate the implementation of cybersecurity system and program requirements for all information systems within their region.

5. Program Administration.

A. The ACIO may assign responsibilities to the Senior Advisor, OT/ICS Cybersecurity, and/or the Associate Chief Information Security Officer (ACISO).

B. The Senior Advisor, OT/ICS Cybersecurity will:

(1) develop and maintain a Reclamation-wide OT/ICS IMT Cybersecurity Program,

(2) provide cybersecurity support to regional and area offices,

(3) serve as the OT/ICS IMT cybersecurity advisor providing support to OT/ICS IMT personnel,

(4) verify compliance with FISMA requirements for Reclamation OT/ICS IMT, and

(5) manage the teams and resources responsible for maintaining the Reclamation-wide OT/ICS IMT Cybersecurity Program.

C. The ACISO will:

(1) develop and maintain a Reclamation-wide enterprise IMT Cybersecurity Program,

(2) serve as the enterprise IMT cybersecurity advisor providing support to IMT personnel,

(3) verify compliance with FISMA requirements for Reclamation enterprise IMT, and

(4) manage the teams and resources responsible for maintaining the Reclamation-wide enterprise IMT Cybersecurity Program.

D. The RISSMs will update regional directors; the Senior Advisor, OT/ICS Cybersecurity; and the ACISO of region level cybersecurity procedures.

E. The ISSO(s) will detail, maintain, and update RISSMs of IMT boundary level cybersecurity procedures.

6. Risk Management.

A. The ACIO is the Authorizing Official with the sole authority to formally assume responsibility for operating Reclamation information systems at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation (see Paragraph 4.J.(1) of RM Delegations of Authority).

B. The ACIO will ensure:

(1) Reclamation's information systems risk management processes are linked to mission risk management processes at the bureau level, and

(2) information system risks are viewed from a Reclamation-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core mission and business functions.

C. The Senior Advisor, OT/ICS Cybersecurity and the ACISO will develop and implement cybersecurity strategies to improve Reclamation's overall security posture and reduce risk.

D. The Enterprise and OT/ICS IMT Security Teams will be cybersecurity advisors to the Senior Advisor, OT/ICS Cybersecurity and ACISO on all matters, technical and otherwise, involving the cybersecurity posture of IMT and the overall effectiveness of implemented cybersecurity controls.

E. The RISSM will be a cybersecurity advisor to the designated region or office and briefs the ISO on all matters, technical and otherwise, involving the cybersecurity posture of IMT, and will develop and deliver regional- or office-level quarterly risk management briefings to ISOs.

F. The RISSM, in coordination with the ISSO, maintains awareness of the overall IMT security posture and notifies the ACISO and ISO of any changes that increase the risk to Reclamation operations, assets, or individuals.

G. The ISSO will be a cybersecurity advisor on all matters, technical and otherwise, involving the cybersecurity of assigned IMT, and will develop and deliver office-level quarterly risk management briefings to the RISSM.

H. All Reclamation employees must agree to adhere to the established Rules of Behavior before accessing Reclamation Information Systems and promptly report potential cybersecurity incidents and breaches.

7. FISMA.

FISMA requires each Federal agency to plan for security by developing, documenting, and implementing a risk-based IMT security program; assign security responsibilities to the appropriate officials; review IMT security controls; and strengthen the use of continuous monitoring. Reclamation's ACIO implements FISMA requirements through the following program capabilities:

A. Requires the use of the NIST Risk Management Framework to ensure cost-effective security protections are commensurate with the risk, based on the application of organizational risk tolerance thresholds, to help officials set priorities and manage risk consistently throughout Reclamation.

B. Develops and implements organizational metrics that provide transparent and actionable views into Reclamation's compliance with FISMA requirements.

C. Ensures the continued effectiveness of all security controls for IMT by verifying compliance with information security requirements derived from organizational missions/business functions, Federal legislation, directives, regulations, policies, and standards/guidelines.

D. Implements change control procedures with special attention paid to security impacts to organizational IMT.

E. Maintains awareness of threats and vulnerabilities via the implementation of continuous monitoring programs.

F. Authorizes IMT prior to operations and periodically thereafter and requires compliance with information security guidelines and mandatory standards developed by NIST.

G. Maintains System Security and Privacy Plans (SSPP) for all Reclamation IMT, against which each information system can be audited. The SSPP, developed by regional ISSOs and RISSMs, must provide implementation details, an overview of the security requirements, and specifies the applicable security controls.

H. Maintains Plans of Action and Milestones (POA&M) to assist in identifying, assessing, prioritizing, and monitoring the progress for mitigating all IMT vulnerabilities. POA&Ms are developed and implemented by the ISSO for their assigned IMT and managed by the RISSM.

I. Conducts assessments of the management, operational, and technical cybersecurity controls to determine the overall effectiveness of the controls; provides an assessment of the severity of weaknesses or deficiencies discovered in the

information system, recommends corrective actions to address identified vulnerabilities, and prepares the security assessment plan and final report.

(1) In the case of an independent security control assessment, the ISO, RISSM, and ISSO will provide required system access, information, and documentation to the assessors.

(2) RISSMs and ISSOs conduct an annual security control assessment of their assigned IMT to evaluate the cybersecurity controls and recommend corrective actions to address identified vulnerabilities in support of Annual Assurance Statement requirements.

8. Training.

The ACISO ensures the Reclamation IMT Security Training Program is effective and implemented in accordance with FISMA and Department requirements.

A. All Reclamation employees must complete IMT training before accessing Reclamation information systems and annually thereafter.

B. Individuals with elevated privileges or significant information security responsibilities must complete annual role-based security training (RBST), in addition to the prescribed IMT training.

C. Individuals that do not complete assigned IMT security training or RBST annually will have their Reclamation network access revoked until required training has been completed.

9. External Audits.

A. External audits test the effectiveness of information security controls, policies, and procedures in protecting Reclamation's information systems and assess compliance with the requirements of FISMA and related Departmental information security policies, procedures, and standards.

B. Reclamation shall comply with all external audit requests from entities such as the Office of the Inspector General; the Government Accountability Office; the Department's Policy, Management, and Budget; and OCIO to ensure that all mission, legal, and regulatory compliance requirements are met.

C. The Reclamation IT Security Audit Liaison shall coordinate all IT security audit related responsive material submissions.

D. All Reclamation staff are responsible for ensuring that external audit requests are coordinated through the Reclamation IT Security Audit Liaison and responded to in a complete and timely manner.

10. Definitions.
IMT cybersecurity terms utilized in this policy are defined in the NIST Internal Report 7298, Glossary of Key Information Security Terms.

A. **Full Visibility**.
Access to any level of detail within Reclamation's IMT which enables the ACIO to exercise authority, oversight, accountability, and control over portfolio management and operations, workforce, budget formulation and execution, and acquisition activities.

B. **Information Management**.
The collection and management of information from one or more sources and distribution of information to one or more audiences. This may involve persons who have a stake in, or a right to, the information. Management means the organization of and control over information activities, planning, structure, processing, evaluating, and reporting in order to meet mission objectives and enable organizations to function in the delivery of information.[2]

C. **Information Management and Technology or IMT**.
IMT activities include the collective definitions articulated in Paragraphs 10.B., 10.D., and 10.E.[2]

D. **Information Technology or IT**.
Includes, but is not limited to, any services, equipment, or interconnected system(s) or subsystem(s) of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by Reclamation; where such services or equipment are "used by Reclamation" if used by the agency directly, or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources. The term "information technology" does not include any equipment that is acquired

[2]Definition is from Departmental Manual 112 DM 24, Appendix B.

by a contractor incidental to a contract that does not require use of the equipment. This definition is based on the definition of IT in the Clinger-Cohen Act of 1996.[2]

E. **Information Technology Resources**.
Includes all Reclamation budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of IT, acquisitions or interagency agreements that include IT, and the services or equipment provided by such acquisitions or interagency agreements. IT resources do not include grants to third parties, cooperative agreements, or Public Law 93-638 contracts, which establish or support IT not operated directly by the Federal Government.[2]

F. **Operational Technology (OT)**.
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

G. **Industrial Control Systems (ICS)**.
General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

11. Review Period.
The originating office will review this release every four years.