# Reclamation Manual

Directives and Standards

**Subject:** Facility Security

**Purpose:** To establish facility security program requirements for the Bureau of Reclamation. The benefit of this Directive and Standard (D&S) is consistent application of security standards and procedures at Reclamation facilities.

**Authority:** Reclamation Act of June 17, 1902 (ch. 1093; 32 Stat. 388; 43 U.S.C. 391) and acts amendatory thereof and supplementary thereto; Critical Infrastructures Protection Act of 2001 (Pub. L. 107-56; 115 Stat. 272; 42 U.S.C. 5195c); Homeland Security Act of 2002 (Pub. L. 107-296; 116 Stat. 2135; 6 U.S.C. 101); Consolidated Natural Resources Act of 2008, Section 513, Bureau of Reclamation Site Security (Pub. L. 110-229; 122 Stat. 755; 43 U.S.C. 373e); Executive Orders (EO) 10450, 10577, 12958 as amended, 12968 and 12977; Homeland Security Presidential Directives 3, 5, 7, 12; Presidential Policy Directives 7 and 21; Federal Information Processing Standards (FIPS) 200 and 201; and Departmental Manual (DM) Parts 442, 444, and 446

**Approving Official:** Director, Policy and Programs (P&P)

**Contact:** P&P, Security Office (84-57000)

1. **Introduction.** The facility security component of Reclamation's security program is concerned with the physical, technical, and procedural systems for assessing, reducing, and managing security-related risks and prescribes minimum security requirements and processes for Reclamation facilities.

2. **Applicability.**

   A. This D&S applies to all Reclamation personnel.

   B. The requirements of this D&S apply to all Reclamation-owned or occupied (defined in paragraph 16.F) facilities and structures, except as defined in paragraph 2.C. Transferred Works (defined in paragraph 16.J) are subject to all requirements, unless stated otherwise.

   C. The requirements of this D&S do not apply to "Very Low Risk (LR)" facilities (described in DM chapter 444, Part 1: *Physical Security Program Requirements* (444 DM 1) and paragraph 16.B (5)), except where specified, or security measures in place exclusively for land management, safety, recreation, or other non-security risk management purposes.

3. **Security Program Management and Staffing.** The following functional roles and requirements are mandatory for successful program management:

   A. **Management**.

      (1) The Chief Security Officer (CSO) will serve as the security program manager (described in 444 DM 1). The CSO will formulate, coordinate, manage, implement, and oversee Reclamation's security program. This includes associated internal control processes, policy development, and facility security risk management (special agent and security guard management, intelligence support, and law enforcement (LE) support). Coordinate with other risk management offices to develop and implement policy and processes (e.g., emergency management, dam safety, and facility operations).

      (2) Regional Directors (RD) will manage and oversee the security program throughout their region to ensure all facility security program requirements and adequate protection measures are in place to safeguard Reclamation personnel and assets.

      (3) Area and facility managers will oversee the daily operation, management, and maintenance of the facility security program. This includes security equipment, security guard forces, security-related contracts, supporting processes, training, and documentation to ensure all facility security program requirements, procedures, and security countermeasures are implemented, maintained, and properly operated in accordance with Reclamation, departmental, and applicable external policy requirements and standards (see paragraph 5).

   B. **Staffing**. The RD will ensure the following staffing is in place to support the security program.

      (1) Each regional office shall have a qualified, full-time regional security officer (RSO) who will be responsible for managing the overall regional security program on behalf of the RD and CSO.

      (2) Regional special agents (RSAs), as defined in the current interagency agreement, will regularly coordinate and interface with other LE and intelligence agencies to maintain relationships for support in security and threat assessments, mission facility response, and criminal investigations. This information will also be used in assisting the RSOs in providing security-related training and keeping regional management informed of security office initiatives.

      (3) An area office security coordinator (AOSC) will be assigned to coordinate and oversee security functions and training, as well as, provide support to the area manager, RSO, RD, and the security office in accomplishing the security program. The area manager will evaluate internal needs to determine if the

AOSC is more appropriate as a collateral duty or assigned to more than one employee.

(4) Each National Critical Infrastructure (NCI) facility will have an experienced, full-time facility security manager who is trained, per departmental and Reclamation requirements, and is responsible for the day-to-day security guard functions and oversight of security activities. The NCI security manager (NCI-SM) position, as defined in Reclamation Manual (RM) D&S, *Security Program* (SLE P01) and 444 DM 1, must be dedicated to the security function; any additional duties must not diminish the primary responsibilities and needs of the security program. The area manager will evaluate internal needs to determine if the NCI-SM will also serve as the AOSC for its area office.

4. **Training Requirements.**

A. **Security Awareness Training**. Security awareness training must be provided annually to all Reclamation employees by the AOSC, RSO, or security office. New employees must complete this training within 60 days of initial employment.

(1) RSOs, in coordination with RSAs and the area office, will develop generic security awareness training materials to address roles and responsibilities (e.g., in relation to the implementation of security program requirements and threat response measures), protocol for observation and reporting of incidents and suspicious activities, and all the required components listed in 444 DM 1. AOSCs will then tailor these generic materials, as appropriate, to specifically address unique facility nuances such as site-specific operational security requirements and issues, tourism security needs, or expectations to support local security or LE emergencies. Materials must be reviewed annually, at minimum, and updated as circumstances require, by the AOSC.

(2) Except for onboarding training, all completed security training must be documented by the AOSC and include topics covered, date, time, names of attendees, and the trainer. This documentation must be made available to the RSO or security office upon request.

(3) All completed security training must be reported by the AOSC within the area office's annual security report and be available for internal control reviews.

B. **Security Professionals.** Refer to 444 DM 1.8 A (Table 1) for the minimum requirements for security professionals, which comprises the CSO, RSOs (both are listed as "Bureau/Office Security Officer/Manager" in Table 1), and the NCI-SMs. This table does not apply to AOSCs or other security office personnel.

5. **Agency-level Security Requirements.** This paragraph contains requirements from the Department and other agencies. These requirements apply to all mission facilities including

LR facilities. Reclamation facility and area managers will implement, operate, and maintain physical and electronic security measures as determined by Reclamation decision documents (see paragraph 8) and applicable Federal policies and standards, including:

A. **DM's Minimum Security Standards.** DM Part 444 prescribes minimum security standards that must be applied to all structures owned or occupied by a departmental office or component and to all persons entering in or on such property. The RSO is responsible for validating facility compliance with the DMs.

(1) **444 DM 1 – Physical Security Program Requirements.** 444 DM 1 outlines requirements and responsibilities for security risk assessments, surveys, and security plans, as well as minimum physical security requirements (e.g., lock and key control, equipment maintenance, identity management, and notification systems). 444 DM 1 is applicable to all occupied Reclamation assets and mission facilities with an Interagency Security Committee (ISC) Facility Security Level (FSL) designation of 1-4.

(2) **444 DM 3 – Closed Circuit Television.** 444 DM 3 outlines requirements for the monitoring, recording, and data storage of video/visual images in areas within and around departmental facilities.

(3) **Other Departmental Manual Requirements.** Refer to departmental requirements such as 753 DM 2 – *Dam Safety and Security Program, Program Requirements*, and the DM Parts 441-446 for more security program requirements.

B. **Threat Condition Protective Measures.** Reclamation's threat condition protective measures are additional security measures implemented based on the Department of Homeland Security's (DHS) National Terrorism Advisory System (NTAS). Reclamation will utilize Appendix A of the DHS Dams Sector Protective Measures Handbook (Handbook), which lists recommended protective measures at each NTAS threat level. The AOSC, in collaboration with the facility manager, area manager, and RSO, will use Appendix A to help determine and document which recommended measures are applicable and appropriate for each facility. Only the response measures planned for usage must be included in a facility's Site Security Plan (SSP). The area or facility manager will, at their discretion, implement additional random anti-terrorism, or other, measures to address a change in local risk factors (e.g., high reservoir levels). The RSO will be notified by the area office whenever additional response measures are implemented.

C. **Federal Information Processing Standards-200.** Facility and area managers will ensure all electronic security systems are designed, procured, installed, and operated in compliance with FIPS-200 requirements. All electronic access control and surveillance systems (EACSS) must be compliant with *FIPS-200, Minimum Security Requirements for Federal Information and Information Systems*. This applies to any EACSS

component that communicates via the Transmission Control Protocol/Internet Protocol, are physically connected to the local EACSS network, are assigned unique IP addresses, and have login capability within the EACSS deployment.

D. **Federal Information Processing Standards-201.** Facility and area managers will ensure all electronic access control systems purchased or deployed by Reclamation after February 19, 2004, are compliant with *FIPS-201, Personal Identity Verification of Federal Employees and Contractors* and related implementing standards, specifications, and guidelines. Design, procurement, and installation of new electronic access control systems or major upgrades to, or replacement of, systems installed before 2004 will be FIPS-201 compliant. This does not apply to Transferred Works, except in locations where an operating entity and Reclamation share a building or office space managed by Reclamation.

E. **Interagency Security Committee Policies, Standards, and Best Practices.** The ISC has several requirements that apply to all Federal employees and facilities.

(1) Facility and area managers will ensure facilities comply with the policies and standards of the ISC issued pursuant to Executive Order (EO) 12977 which currently includes:

(a) *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (ISC-RMP),*

(b) *Items Prohibited from Federal Facilities: An Interagency Security Committee Standard*, and

(c) *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide.*

(2) At sites with armed security personnel, per 444 DM 1.8 D (5), facility and area managers will apply the ISC's *Best Practices for Armed Security Officers in Federal Facilities* based on the agreed-upon needs as determined by the CSO, RD, and area manager.

F. **North American Electric Reliability Corporation (NERC) – Critical Infrastructure Protection (CIP) Standards.** Supporting the Bulk Electric System (BES), NERC-CIP (further defined in Paragraph 16.E) standards contain minimum requirements for the protection of BES cyber systems (BCS). Facility and area managers will ensure all security systems used to protect all impact-rated BCS and transmission substations and stations, identified under NERC-CIP, are compliant with applicable Reclamation NERC-CIP requirements.

6. **Security Criticality Designations.**

A. FSL designation is required, per 444 DM 1, for all occupied and mission sites (all other assets will be designated as LR). The FSL designation replaces previous programmatic security criticality designations for mission sites (e.g., NCI-LR), used by Reclamation to characterize the relative criticality of all Reclamation dam facilities. The area or facility manager shall make a determination to maintain former LR designations, per the allowed exemption, or to adopt the new FSL 1-4 designation for mission sites, also called M1-4 (further defined in paragraphs 16B and D.).

(1) NCIs are designated as FSL 4, per 444 DM 1.8 B, but also maintain their NCI designation. The current list of NCIs is maintained by the Department and included within 444 DM 1.

(2) Any future change in FSL or LR designation must be made by the region or Security office through a formal decision document (per paragraph 8) which must include a recommendation of a new designation and a justification.

B. A facility's designation applies to all critical mission assets at that facility. In circumstances where this is not appropriate, a breakdown of the assets and their differing designations must be documented in a decision document (per paragraph 8). To ensure inclusion within security program processes (e.g., risk assessments), Reclamation-owned assets outside of the facility's footprint but critical to the mission of the facility must be included as an official asset. If an asset is critical to multiple facilities, then it will only be listed as an asset to the highest-designated facility. For instance, a communication building that services one FSL 3 and multiple FSL 1 and 2 facilities will only be an official asset to the FSL 3 facility. If an asset services more than one highest-designation facility the RSO will determine which facility will list it as an official asset.

C. The official criticality designation and asset lists must be periodically reviewed and updated by the RSO, reported to the security office as changes occur, and, upon request, checked for ISC compliance or other internal control checks by the security office. At a minimum, this will occur every 5 years.

D. The security office will maintain a master security inventory that includes FSL designations.

7. **Security Assessments.** The security office will maintain a security assessment program that ensures security reviews are periodically completed for all FSL 1-4 facilities. Refer to 444 DM 1.8 C for departmental assessment requirements and paragraph 8 for signatory requirements.

A. **Assessment Type and Frequency.** The following table lists assessment types and their required frequency for each facility type. Descriptions of the assessment types and associated requirements follow this table.

| | Facility Applicability | Assessment Type | Minimum Required Frequency |
|---|---|---|---|
| **Required Periodic Reviews[1,2]** | FSL 3-4 mission sites | Comprehensive Security Review (CSR) | Every 3 years |
| | FSL 1-4 mission sites | Periodic Security Review (PSR) | FSL 4: Annually<br>FSL 3: Every 3 years<br>FSL 1-2: Every 5 years |
| | FSL 1-4 mission sites | Annual Security Equipment Inspection (ASEI) | Annually |
| | FSL 1-2 Occupied Buildings | ISC-RMP Facility Security Assessment (FSA) | Every 5 years |
| | FSL 3-4 Occupied Buildings | ISC-RMP FSA | Every 3 years |
| | FSL 1-4 | Internal Control Reviews | Annually (also, as needed, in support of oversight and program management) |
| | All sites with Guards | Guard Effectiveness Assessment | FSL 3-4: Every 3 years<br>FSL 1-2: Every 5 years |
| **Supporting Assessments** | All | Risk Analysis (numerical rating of relative asset risk) | For each CSR and as needed |
| | | Threat Assessment | For each CSR, annually Reclamation-wide, and as needed |

B. **Comprehensive Security Review.** A CSR is used to evaluate potential risks to the public and Reclamation staff and facilities resulting from unauthorized activity by malicious or criminal actors. The CSR reviews security measures and procedures in place, potential threats, structural and procedural vulnerabilities, and consequences of loss (e.g., loss of life and economic losses). The resulting assessment and risk analysis are used to identify appropriate risk-reducing actions and provides a relative priority for

[1] Facilities or critical assets added to the security program inventory must have an initial assessment to determine the FSL, appropriate measures, risk management strategy, compliance status, and any needed fortifications or procedural adjustments. For facilities added to the inventory, that meet the "occupied" definition but do not have mission assets or functions, the ISC-RMP process will be accomplished by the RSO per 444 DM 1. For added mission facilities or assets, regardless of FSL, the security office will complete a CSR. The results of this initial assessment will be documented in an assessment report.

[2] Assessment documents must have all required signatures (per paragraph 8) by September 30th for the assessment to be documented as an accomplishment in current fiscal year annual reporting.

funding mitigation activities. Frequency requirements are indicated in the previous table.

(1) The CSO, or designee, is responsible for ensuring CSRs are done and will assign a CSR team lead for each review. Each CSR team will include a physical security specialist, a facility representative, AOSC (or area office designee), and the RSO (or a team lead approved designee). The CSO will determine appropriate additional personnel from the Security Office, regional office, area office, and facility (including Transferred Works personnel) for the CSR team.

(2) The security office will schedule CSRs to ensure review requirements are met. The PSR is conducted by the RSO as a preparatory step for the CSR site visit.

(3) A CSR is not required on a regularly scheduled basis for FSL 1-2 or LR facilities. However, a CSR will be conducted if a PSR, or other review, determines it is needed or at the request of the CSO or facility, area office, or regional management.

(4) The CSR does not satisfy the requirement for a security equipment inspection (see paragraph 7.D).

(5) A CSR will include a compliance check, review, and update of the previous CSR, risk analysis, and all outstanding security recommendations. Each CSR requires a site visit.

(6) A formal risk analysis for mission assets using the security risk analysis template (located on the security SharePoint site) will be completed by the CSR team lead. This analysis will be completed no later than 30 days prior to the site visit.

(7) RSAs, as defined in the current interagency agreement, will provide the security office with an understanding of: LE response capabilities (resources, timeframes, skills, etc.), site familiarity of responding law enforcement agencies, collaborative relationships with facility management and other responders, exercise participation, and any other pertinent topics or issues. At least 45 days prior to the site visit the RSA is responsible for collecting local threat assessment information and data and provide it to the security office's Intelligence Support (IS) team for integration into the formal threat assessment report. If no RSA is available, the RSO will cover these duties.

(8) The IS will provide a draft threat assessment, at least 2 weeks before the CSR site visit, for the Reclamation site/area being assessed detailing the most likely, worst case, and programmatic threat areas of concern.

(9) CSR findings, including any recommended mitigation actions, will be documented in a report by the team lead. Each recommendation will include the

projected cost, funding source, a viable target completion date, and responsible party.

(10) Upon the completion of the site visit, leadership will be briefed by the CSR team on the assessment's observations and recommendations. If any items identified warrant additional discussion or resolution, the security office will assemble a security advisory team (SAT) including the team lead, CSO (or designee), RSO, AOSC, facility or area office manager (or designee), and other essential staff. The recommended decisions made by the SAT will be documented within the CSR report and serve as the decision document transmitted to approving officials. A SAT is not required if the briefing and completed report are accepted without objection. If the CSR team and SAT cannot resolve the issue(s), the report must include a recommendation to address the unresolved issue(s) by conducting a Security Issue Evaluation (SIE) or Security Corrective Action Study (SCAS).

C. **Periodic Security Review.** A PSR is used to evaluate the security measures and practices in place with respect to the operational effectiveness, utilization, and maintenance of security system equipment and to gauge consistency with security procedures in the facility's SSP. This process will identify any security concerns requiring additional assessment or review. The PSR is not intended to address significant issues or make formal recommendations; however, any identified issues requiring funding must be documented within a decision document (per paragraph 8).

(1) The RSO is responsible for ensuring the accomplishment of all scheduled PSRs each year. Frequency requirements are included in the previous table.

(2) In years when a CSR is also being accomplished, the PSR will be completed by the RSO at least 2 weeks before the CSR site visit. The security office will establish and maintain the annual PSR schedule.

(3) A PSR will consider prior facility reviews, evaluations, and outstanding recommendations. A site visit is encouraged but not required for PSRs.

(4) PSRs must be documented using the most recent template available from the security office. The RSO will ensure all PSRs are signed, and subsequently posted on the security SharePoint site, by September 30th of the current fiscal year.

(5) If it is determined that a more detailed risk assessment is needed, it will be documented (via e-mail, memorandum, or decision document), including the reason for the detailed assessment request, proposed type of assessment, and proposed schedule for completion, by the RSO and sent to the CSO, area manager, and AOSC.

D. **Annual Security Equipment Inspection.** All security equipment will be annually accounted for and inspected to ensure it is operating properly. This ASEI is conducted

by the AOSC as an oversight function but can be accomplished by others as directed. The ASEI will be documented by the lead and provided to the facility manager, who in turn, will ensure any issues affecting the operation or stability of the security systems are properly scheduled for mitigation. The date and findings of the ASEI, as well as any corrective actions, must be reported by the AOSC in the area office's annual security report.

E. **ISC-RMP Facility Security Assessments.** 444 DM 1 requires Department bureaus and offices to use the DHS's ISC-RMP for conducting FSAs at departmental occupied facilities. The approved ISC-RMP security standards must be in place at the facility during the time of occupancy.

(1) The ISC-RMP is required for facilities, dams, and other mission structures (e.g., power plants and control centers) occupied by Reclamation employees as defined in paragraph 16.F.

(2) All assets occupied by Reclamation employees must have periodic FSAs as shown in the previous table. The RSO, or designee, will conduct the FSA, per the latest ISC-RMP guidance, and collaborate with the facility and area office manager to ensure the assessment accurately reflects the asset (including Transferred Work assets) and its risk management needs.

(3) The RSO, in consultation with area office and facility personnel, ensures Reclamation is represented on each multi-tenant facility's Facility Security Committee and the ISC-RMP review is accomplished per ISC-RMP requirements.

(4) Details of the ISC-RMP review, including justifications for not implementing a recommended standard, must be documented utilizing the latest Reclamation ISC-RMP FSA template available from the security office.

(5) The RSO will ensure all FSAs are signed, and subsequently posted on the security SharePoint site, by September 30th of the current fiscal year.

F. **Internal Control Reviews.** At the discretion of the CSO, the security office or RSO will conduct oversight reviews at the regional offices or facilities to ensure all requisite security standards and procedures are implemented and detect and prevent errors, fraud, waste, and abuse. The security office's annual internal control program summary document (PULSE) contains performance measurements for each program area within the security office (e.g., Personnel Security, IS, Risk Assessments, RSOs, RSAs, Information Security, Studies).

(1) Each program lead will develop and maintain, on the security office SharePoint site, a compliance checklist which will be used during internal control reviews. This checklist will be based on the program area criteria outlined within PULSE.

(2) Each program lead will conduct at least one annual internal control review. Internal control reviews must be documented and include:

(a) name and title of reviewer,

(b) date of review,

(c) references to PULSE measure(s) being reviewed,

(d) results summary and non-compliance findings, and

(e) recommended mitigating action items (if any).

(3) Each program lead will summarize and submit internal control review findings to the CSO using the PULSE template by September 30th each year.

(4) In addition to PULSE reporting, each RSO will annually conduct an oversight review of at least one facility from the region's security inventory per paragraph 7.I.(4). Each review will include a full compliance check of departmental and Reclamation requirements.

G. **Security Issue Evaluation.** A SIE is used to evaluate a specific security issue and potential mitigation alternatives. Issues requiring a SIE are typically identified through a security assessment, but are also potentially triggered by risk factor surveys, security-related incidents, exercises, general research, or proposed changes to previous decisions or security posture. The RSO will maintain communications with the facility and area office to ensure any identified issues are properly submitted using the SIE process. SIEs, and resulting reports, vary in size and resource needs depending on the scope and complexity of the issue.

(1) For large or complex evaluations, a SIE project team will be established by the project team leader to plan, manage, and accomplish the SIE. The project team leader will generally be from the area or regional office where the project is located.

(2) The SIE team will, at a minimum, include the RSO and other Reclamation staff needed to accomplish the study.

(3) A SIE decision document will be prepared by the team conducting the evaluation and submitted to the security office for review and signatory approval per paragraph 8. At a minimum, the decision document must include a detailed summary of the issue, discussion of the alternatives (including pros and cons), estimated risk reduction or benefit from completing identified alternatives, cost, and a recommended decision and supporting justification to either rely on current security measures in place (take no action), implement specific mitigation actions, or conduct a more in-depth SCAS.

H. **Security Corrective Action Study.** A SCAS is used when a comprehensive analysis of security-related issues and mitigation alternatives (e.g., structural modification), is needed. The SCAS includes engineering designs, cost estimates, projected risk reduction, and environmental impacts. A SCAS must be initiated through a decision document (per paragraph 8) with a justification. Refer to the SCAS Guidelines on the security SharePoint site for more information.

I. **Other Supporting Reviews and Activities.** The following tasks provide supporting information and data for security reviews and activities.

(1) **Risk Analysis.** A security risk analysis evaluates the perceived threats, vulnerabilities, consequences, and security measures at a facility. It provides a relative risk rating for each critical facility asset. This rating is used to prioritize Reclamation-wide mitigation activities and to provide a relative quantification of risk to aid decision makers in determining if a mitigation action is warranted for a specific asset. The risk analysis is conducted, reviewed, and updated by the security office staff, in collaboration with regional and area office staff, prior to CSRs, SIEs, SCASs, or as changes occur that might affect the risk rating of a facility. The risk analysis will be updated after significant mitigation activities have been completed at a facility. A formal risk analysis will be completed by the CSR team lead per paragraph 7.B.

(2) **Threat Assessments.** A threat assessment evaluates potential security-related threats to a facility, including potential types of attack, aggressor capability, and perceived intent. These assessments are based on a combination of local, regional, and international threat and intelligence information. Threat assessments are accomplished to support risk assessments (see paragraph 7.B) or in response to critical intelligence indicators or management concerns. The IS will provide an annual Reclamation-wide threat estimate which is a near-term perspective of tactics and trends and their potential impacts to mission and operations. Local threat assessment information will be collected by the responsible RSA, as defined in the current interagency agreement, or RSO, and provided to the IS for integration into the final threat assessment.

(3) **Technical Visits.** Site visit requests (e.g., technical site surveys or site assistance visits) that require members of the security office staff, must be approved by the CSO. These visits will be documented by the team lead in a trip report and distributed to the facility, security office, and other management based on the purpose and findings.

(4) **Program Integration and Management Activities.** Periodic collaborative activities must be conducted by the RSO and area office to ensure security processes are being integrated and managed at the facility. These activities are for the purpose of collaboration and oversight and do not require any formal documentation.

(a) RSOs must administer the security program within their assigned region(s) by planning, developing, implementing, and overseeing appropriate levels of physical, operational, personnel, and information security for all Reclamation-owned facilities as determined collaboratively with the CSO and regional management. This oversight will include regular reviews and collaborations at facilities to ensure effective management and implementation of the following programmatic areas:

(i) funding account management,

(ii) policy compliance,

(iii) security-related contracts,

(iv) security-related training for employees and security and LE professionals,

(v) information and operations security,

(vi) facility security response, SSP, and other tools for effective emergency management and response,

(vii) access control including facility security, identity management, and personnel security,

(viii) guard program effectiveness, and

(ix) technical oversight and support of security-related activities of the AOSC.

(b) The area office will integrate the site's security program into other facility programs and processes (e.g., operations and maintenance (O&M) schedules, emergency management, and continuity operations) to ensure security risks are effectively managed and responded to by all employees. The area office will conduct periodic reviews (e.g., maintenance priority schedules or facility response exercises) to determine how effective security is being integrated into normal processes and programs.

J. **Recommendation Tracking.** All risk assessment recommendations will be tracked in a database maintained by security office staff. A recommendation tracking report will be sent to each region on a semi-annual basis (September and April). The area office or facility will update the status of recommendations and provide the updated data to the security office within 30 days of receipt.

K. **Risk Assessments by External Entities.** All requests for an external security assessment of a Reclamation facility must be submitted, in writing, to the CSO. The CSO will approve requests after consultation with the RD and area manager.

8. **Decision-Making Process.** Security measures at Reclamation facilities are collaboratively determined through a formal risk assessment or decision-making process and are approved in formal decision documents. These processes are described below and in paragraph 7.

A. **Decision Document.** A security decision document can be created by any Reclamation employee and must be signed as indicated in paragraph 8.B. A decision document is required to: approve security funding for implementing a recommendation or study, change a criticality designation, change the intent or decision on an existing recommendation, change public tours or visitor access, or make a change in security strategy or posture (e.g., guards or physical security measures) at a mission asset. If there is a decision warranting action and requires funding from the security office, the decision document will describe the recommended mitigation action, final decision, supporting justification, timeframes, estimated cost, funding sources, and responsible office for implementing that recommendation. If a decision is made to take no action, then that decision will be documented with supporting justification. CSR, SIE, and SCAS assessments do not require a separate decision document if they include all relevant information described in this section and signatures from the area manager, RD, and CSO.

B. **Concurrence Levels.** Security decision documents require signatory concurrence at the following levels[3]. Electronic signatures are acceptable.

| | Mission Sites | Area Manager[1] | Regional Director[1] | Chief Security Officer[1] | P&P Director[1] | Deputy Commissioner PAB[2] | Commissioner and AS/WS[3] |
|---|---|---|---|---|---|---|---|
| CSR | FSL 3-4 | ✓ | ✓ | ✓ | | | |
| SIE | FSL 1-2 | ✓ | ✓ | ✓ | | | |
| | FSL 3-4 | ✓ | ✓ | ✓ | ✓ | | |
| SCAS | FSL 1-2 | ✓ | ✓ | ✓ | ✓ | ✓ | |
| | FSL 3-4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Other[4] | All | ✓ | ✓ | ✓ | | | |

[1] Document can be signed by a deputy manager or director
[2] Policy, Administration, and Budget
[3] Assistant Secretary for Water and Science

[3] The CSO is delegated the authorities contained in 441-444 DM and paragraph 4 of the RM Delegations of Authority release.

[4] "Other" includes decision documents (e.g., decision memorandum)

9. **Consultation with Project Beneficiaries.**

A. All security-related consultation requirements of Public Law 110-229, Section 513 are accomplished by the regional or area office responsible for the facility. The RSO, with the assistance of the security office, will provide technical information and support regarding the need for the site security measure(s) and estimated costs.

B. Upon identifying a new site security measure, the area manager will provide project beneficiaries, who have a direct responsibility to repay project O&M costs, a notice and consultation opportunity. Costs for consultation are assumed by the project beneficiary.

C. If project beneficiaries participate in a security assessment that generates site security measures the requirements for the notice, consultation, and response stated in paragraph 9.B are met.

D. Emergency situations or elevated threat condition changes increase the levels of physical security protective measures and do not require prior notice and consultation under Pub. L. 110-229, Section 513. Area managers are responsible for communicating the impact of sustained emergency measures to regional leadership, the CSO, authorities, and beneficiaries, as soon as possible.

10. **Security System Design, Operation, and Maintenance.**

A. **Design of Security Systems.**

(1) **Consistency with Decision Documents.** The area and facility manager are responsible for ensuring all security system designs and equipment commensurate with the approved recommendations in risk assessment decision documents, as well as with other applicable requirements (e.g., Federal and departmental policies, D&S, facility security requirements). New security systems or equipment will not be installed, or existing systems significantly upgraded or modified, without an approved decision document as described in paragraph 8. At Transferred Works, security equipment installed will be consistent with the security strategies and mitigation measures established in Reclamation's security risk assessments of the facility.

(2) **Integrated Design.** The area and facility manager, and all employees will ensure physical and technical security measures and systems are integrated, to the greatest extent possible, into a facility's design processes and operating systems. Security measures (e.g., access control systems, automatic gates, video monitoring systems, intrusion detection systems, and command and control systems) will be, wherever possible, integrated into a single, operator-friendly system by the facility manager in coordination with the RSO or the security

office. The design process will consider the feasibility of integrating the monitoring function of any new or upgraded security system, with the monitoring capability of existing security systems, that provide continuous monitoring, assessment, and dispatch functions, either at a government or commercial central monitoring station. For Transferred Works, where new measures and systems are a part of, or contiguous with, operating entity security measures and systems, design integration requires close cooperation between the area office and operating entity. For construction activity on a high or significant potential hazard dam, the area and facility manager will ensure the RSO is consulted for security concerns and the designs are reviewed in accordance with FAC 03-02 for risk neutrality.

(3) **Design Approval.** Upon decision document approval, the design specifications for security systems, funded by the security office, must be reviewed and approved via email by the security office's lead physical security specialist before the procurement process is initiated. It is highly encouraged that all security system designs, regardless of funding, be reviewed by the security office. Reviews will help ensure: the intent of the recommendation is being met, components are compatible, there is a positive track record for reliability, maintenance, and ease of operation, compliance with applicable industry, federal, departmental, and Reclamation physical security standards and information technology (IT) compliance requirements, and adherence to cost-effective procurement and O&M strategies.

B. **System Components**.

(1) P&P physical security specialists will be consulted before replacing security system components, unless identical components are available or have been previously approved. This includes components of access control systems, vehicle and boat barriers, video monitoring systems, intrusion detection systems, and other security-related products. The consultation will determine if P&P can provide funding from the replacements budget and ensure replacement equipment is the most effective and cost efficient product available and the proposal complies with applicable industry, Federal, departmental, and Reclamation physical security and cybersecurity requirements.

(2) All security system devices must be purchased in accordance with Executive Order 13873 - Securing the Information and Communications Technology and Services Supply Chain, and Executive Order 13920 - Securing the United States Bulk-Power System, which prevent the purchase of information technology equipment from nations which are adversarial to the United States. Security system device purchases should obtain the proper vendor origin verification approvals through Reclamation's IT purchasing process. In addition, all security system devices need to follow Reclamation's Federal Information Technology

Acquisition Reform Act (FITARA) program and obtain the necessary IT approvals prior to being purchased.

(3) All security system devices must also be purchased in accordance with the National Defense Authorization Act of 2019, Section 889, which prohibits the purchase of telecommunications and surveillance equipment from specific vendors and which contain certain processing units which have known vulnerabilities.

C. **Operations of Security Systems.** The facility manager, or designee, is responsible for the proper operation and utilization of all security systems and associated equipment. This includes ensuring:

(1) All current or planned equipment will be used to maximize security effectiveness, to include proper monitoring and prompt assessment and response.

(2) Security alarms at FSL 2-4 mission sites are monitored at a central station with notification to LE or security responders, unless otherwise approved using the normal decision-making process (see paragraph 8). A documented protocol will be developed by the NCI-SM, or designee, to ensure alarms are assessed immediately, taking priority over non-urgent operations. This documentation must be made available to the RSO or security office upon request.

(3) Security system alarm and error logs, or automated reports generated by the security system, are reviewed by the NCI-SM, or designee, to ensure any EACSS issues requiring maintenance, repair, or procedural/training adjustments have been identified, documented, and sent to the proper office, or person, to have the issue(s) corrected. These logs or reports must be reviewed regularly in accordance with documented policies and procedures. All system issues and anomalies will be documented in the facility's normal O&M management system, investigated, and corrected in a timely manner by the NCI-SM to prevent any increases in security risks.

(4) A summary of significant outages, failures, and corrective actions taken must be documented by the facility manager as they occur and included, by the AOSC, in the area office annual security report (see paragraph 11.B).

(5) As-built security drawings must be maintained by the facility manager, or designee, for critical security components and systems in the area.

(6) The NCI-SM, or designee, will complete and maintain an equipment inventory of all EACSS system components or critical items (alarm controller panels and communications equipment (e.g., media converters, hubs)) to ensure ASEIs and performance testing are completed on all security equipment. Non-critical, consumable, and easy to procure, low-cost commercial-off-the-shelf (COTS)

equipment (less than $5,000) do not need to be inventoried. Examples of low-cost COTS equipment include surge suppressors, fuses, and power supplies.

D. **Maintenance of Security Systems.** The facility manager, or designee, is responsible for ensuring all security systems and equipment are properly maintained, tested, repaired, and replaced, as needed, to maintain the security mission of the facility. 444 DM 1 includes additional requirements for security equipment maintenance. Contact the security office for additional guidance on maintenance and replacement of security equipment and associated frequencies. The facility manager will ensure:

(1) All equipment is maintained, in good working order, to maximize security effectiveness and longevity (e.g., cleaning and calibration of cameras, maintenance of the lock and key control program, or physical barrier maintenance).

(2) Performance testing of security equipment is conducted by the NCI-SM, or designee, to ensure functionality and effectiveness. All security equipment will be tested annually per 444 DM 1. The performance tests will be performed using the Reclamation Power Equipment Bulletin (PEB) 59 and individual component Technical Orders or manufacturer specifications. The performance testing will be documented and routed through the facility manager and the area office's O&M position in charge of facility maintenance for concurrence. Any significant findings will be reported in the area office's annual security report.

(3) Preventive maintenance inspection/procedures (PMI) must be conducted annually on all security equipment by the facility manager, or designee, to ensure all are operating nominally and within manufacture specifications (see PEB 59 for additional guidance). The PMIs will be documented and routed through the person in charge of facility O&M and the AOSC for concurrence. Any significant findings will be reported in the area office's annual security report.

(4) Equipment malfunctions or outages are immediately reported to facility maintenance staff or entered into maintenance tracking systems following facility procedures. If failure of any security system critical component at an FSL 3-4 creates a significant vulnerability to mission assets or personnel, the facility must notify the area manager immediately, and the RSO within 24 hours. Reporting for equipment issues at an FSL 1-2 will be at the discretion of the area manager. Compensatory measures (e.g., measures that ensure equivalent security capabilities without any increase in risk) must be implemented immediately for all security mission critical equipment (see paragraph 16.G) or within 72 hours for all other equipment. The compensatory measures must be maintained until the equipment is back in full service. The area manager will ensure the RSO is briefed on the nature and impact of compensatory measures. The RSO will communicate with the CSO and regional management.

(5) All security equipment is integrated into the facility's normal operations, maintenance, and replacement programs. These include normal scheduling of preventative maintenance, semi-annual performance testing, ASEI dates, and equipment replacement in the facility's normal O&M management system.

(6) Potential funding assistance needs notifications go to the RSO and the security office to accommodate major upgrades or replacements for security systems or components that have exceeded their end of useful service life (see paragraph 10.E.(7) and RM D&S, *Reimbursability of Security Costs* (SLE 05-01)). SLE 05-01 covers budgeting and reimbursability of O&M costs. This notification must take place with enough time to properly plan and budget for such investments (fiscal year prior or at least 6 months from the defined date of need).

(7) Spare security equipment:

(a) FSL 3-4 mission sites will maintain spare equipment of EACSS system components or critical items. Spare equipment levels will equal 10 percent of the total or at least 1 of each piece of equipment, whichever is greater. Critical system components include any detection, access control, and surveillance devices that if damaged, destroyed, or otherwise compromised would: undermine a substantial or critical portion of the system, have a significant effect on the sites ability to perform its mission, or require the implementation of compensatory measures.

(b) FSL 1-2 mission sites will keep one spare of each EACSS system component or critical item.

(c) The facility does not need any spare equipment for perishable technologies (equipment where the technologically relevant lifespan may be shorter than its useful service life).

(8) End of useful service life:

(a) End of useful service life shall be calculated from the date of installation. For useful service life durations refer to SLE 05-01, Appendix A – *Service Lives for Security Equipment*.

(b) Per NIST SP 800-53, Security and Privacy Controls for Systems and Organizations, Security Control SA-22, IT components must be replaced prior to becoming end-of-life when the vendor stops supporting it, regardless of site criticality level, operational status, or system type.

(c) Non-perishable items that have reached the end of its useful service life and are still in serviceable condition will remain in service. All equipment will be inspected for potential issues during the performance of preventative maintenance and functional testing. System review and replacement will

take place as needed, or at the end of a pre-determined life-cycle, based on preventative maintenance reports, recommendation of facility manager, or reviews performed by the RSO or security office.

(d) Perishable technologies will be replaced at the end of their useful service life, regardless of site criticality level, operational status, or system type. Perishable technologies include, but may not be limited to:

(i) servers,

(ii) workstations (e.g., personal computers, desktop clients),

(iii) routers/switches,

(iv) networked video recorders, and/or

(v) digital video recorders.

(9) The area office responsible for Transferred Works will ensure the O&M plans and documentation, maintained at the area office and the operating entity, collectively address the aforementioned O&M requirements and are available to the RSO and CSO upon request.

11. **Signage.** The facility manager of an FSL 1-4 site will post See-N-Say signs and restrictive signage (e.g., No Trespassing, Restricted Area, Surveillance Cameras in Use, Unmanned Aircraft Systems, Restricted Air Space) in public areas, perimeters, and likely avenues of approach. Templates for security program signage are available from the security office.

12. **Additional Reporting Requirements.**

A. **Reporting Risk Concerns.**

(1) All employees must report any changes that could potentially affect security risks to the facility manager. The facility manager must report changes to the AOSC.

(2) AOSCs must maintain awareness of the risks at their respective mission facilities and report any significant or potentially significant changes in risk to the RSO. The RSO must then determine the need to report these changes to the security office for revision in risk analysis numbers, security measures, or overall risk management strategies.

(3) RSOs and RSAs, as defined in the current interagency agreement, will immediately communicate information on threats and incidents that could affect the security of Reclamation facilities to the area and regional security personnel, CSO, IS, and senior leadership (e.g., RDs, deputy managers, supervisors).

(4) RDs must keep the P&P Director informed of significant facility security issues and decisions such as road closures and openings, major security training exercises, major changes in security posture, guard, patrol, monitoring, or other protection services, major changes in risk factors, mission, or public use, or significant changes in visitor tours.

B. **Area Office Annual Security Report.** The requirement for an area office annual security report is described in RM D&S FAC 01-06 *Annual Reporting for Dam Safety, Security, and Related Operations* (FAC 01-06) and in 444 DM 1.9 C.

C. **Facility Security Plans.** The ISC-RMP requires a written facility security plan for all FSL 1-4 occupied structures. The RSO will ensure all occupied structures are compliant with the latest ISC-RMP plan criteria and requirements.

D. **Site Security Plan.** An SSP must be developed, by the area office in collaboration with the RSO and the facility, for all unoccupied FSL 1-4 mission facilities. SSPs and specific plan components are defined in 444 DM 1. The area office must coordinate with Transferred Works to ensure effective SSPs are developed and maintained for each facility.

(1) The SSP must be used in conjunction, and avoid contradictions with, Standing Operating Procedures (SOP) and the Emergency Action Plans (EAP). The SSP can be integrated into the SOP, EAP, or other facility response documents.

(2) The area office will support a coordinated response by ensuring SSPs and other security response-related documents and protocols are annually reviewed and updated to ensure response measures are adequately defined and up to date, contact information is accurate and complete, and information is consistent with EAPs and SOPs. Additionally, the SSP must be exercised (every 3 years for FSL 3-4 mission sites, every 5 years for FSL 1-2 mission sites) to ensure it accurately reflects the site's capabilities (e.g., measures, resources, equipment, and materials) for response. These SSP activities and findings will be annotated in the area office annual security report.

(3) SSP templates and checklists are available on the security SharePoint site or from the RSO. All components within the template must be addressed including, but not limited to, the signature and revision pages. SSPs must be initially reviewed by the RSO to ensure completeness and accuracy. A copy of the signed SSP and any revisions will be uploaded, by the area office, to the security SharePoint site.

(4) The area office will ensure the SSP is used for real world events and to develop security program objectives, injects, exercises, drills, and tests, as part of the EAP exercise program per RM D&S FAC 01-01 *Emergency Action Planning Program for High- and Significant- Hazard Dams (and other facilities, as applicable)* (FAC 01-01). The area office will update the SSP to reflect lessons learned from each EAP or real world or exercise events.

E. **Emergency Action Plans and Exercises.** The EAP is a formal document that identifies potential emergency conditions at a dam and specifies pre-planned actions to minimize property damage and loss of life. Refer to RM D&S SLE 08-03 *Serious Incident Reporting and Duty Officer Program,* for exercise guidance. Requirements for EAPs are in FAC 01-01. Security objectives and potential scenario information and outlines are available from the security office. Since there are several security scenarios by which potential emergency conditions could occur, the following requirements apply to the AOSC and RSO in regard to the EAP program.

(1) The AOSC must coordinate with the area office EAP coordinator to ensure a facility's EAP integrates security information as it pertains to the purpose and scope of the EAP event (e.g., the notification contact list for security and response personnel).

(2) The AOSC and RSO must collaborate with the EAP coordinator on exercises for all FSL 1-4 mission sites and all non-mission FSL 3-4 sites to determine an opportunity or need for inclusion of security components/scenarios. This includes participating in the planning and conduct of exercises to provide collaborative integration of security response activities, as deemed appropriate by the area manager. Any security-related information and recommendations resulting from the exercise will be documented by the RSO.

(a) The RSO will notify the Protection Services Program Manager regarding security response aspects of exercises and findings.

(b) Recommendations requiring funding by the security office must have a decision document per paragraph 8.

(c) The RSO will implement and track security recommendations and ensure any updates to the SSP and security program are completed.

13. **Visitor Centers, Tours, and Foreign Visitors.** The following requirements apply to Reclamation personnel managing tours, visitor centers, and foreign visitors. Individuals accessing a non-public area must be screened, display a temporary/visitor badge, and be escorted at all times. The AOSC must document security requirements and processes for each tour that visits a critical mission asset.

A. **Visitor Centers.** Reclamation's RM Policy LND P13 *Visitor Center Policy, Directive and Standard, and Guidelines,* contains information on tour and visitor center security. These guidelines must be considered when designing or changing public tours and visitor centers to integrate security designs, procedures, and best practices and ensure the safety and security of visitors, employees, and facilities.

B. **Public Tours.** All changes to public tours that have a significant security-related impact require a decision document. More complicated issues will undergo the SIE process (see paragraph 7.G) at the discretion of the CSO. Area offices are responsible

for providing all tour guides and visitor center personnel initial and biennial training in security awareness and tourism security.

C. **Non-public Tours.** Hosting offices must schedule all non-public tours (e.g., school groups, technical groups, and international groups) with the facility in advance, obtain a list of tour participants, determine the tour route and information, and notify the RSO and area office. The RSO has additional guidance for non-public tours of Reclamation facilities.

D. **Foreign Visitors.** For additional requirements for visits by foreign nationals, see RM D&S NIA 01-01, *Reclamation's International Affairs Program,* which covers Native American and International Affairs Office reporting requirements.

E. **Funding.** Funding for visitor centers, tours, or other public services cannot be sourced from security funding appropriations and must come from other sources. Security equipment that provides a direct benefit to the facility can be funded if approved by the formal decision process (see paragraph 8).

14. **Security Guards.** Refer to the 446 DM series and the RM D&S SLE 04 series for additional security guard requirements.

A. **Changes.** Before implementation of any substantial changes to guard force configuration or manning strength the AOSC/NCI-SM will go through the SIE process (see paragraph 7.G) for any FSL 3-4 site(s).

B. **Effectiveness Review.** Per 444 DM 1.8 D (5), the Protection Services Program Manager and the RSO will conduct an effectiveness assessment of the guard program every 3 years.

C. **Contracts.** At least 18 months before contract award or renewal, the AOSC/NCI-SM will ensure contract and work plans for armed and unarmed proprietary (employed solely by Reclamation) and contract guards receive concurrence from the RSO and security office. See 444 DM 1.8 D (5) for additional requirements. Reclamation-wide facility security program standards and example contract language are available from the security office.

D. **Exercises and Drills.** The area manager is responsible for ensuring security guard exercises and drills are integrated into the security training program. Refer to 444 DM 1.8 D (5) and the 446 DM series for additional requirements.

(1) The NCI-SM will ensure NCI facilities, and those with on-site security guards, conduct a full-scale security exercise to review, evaluate, and test established guard force interaction and interoperability with security systems and facility operations in response to specified scenarios every 5 years. The intent is to test the designated guard force protocol, evaluate their understanding of expectations, gauge training and operational gaps, identify needs for equipment or protocol

improvements, and test the ability to mitigate reasonable security or LE emergencies that endanger the mission or life-safety of personnel.

(2) Security exercises and drills will not incorporate any practical application of use-of-force without the express, written approval of the CSO. Evaluating the simulated practical application of significant or potentially deadly force (e.g., drills using Simunition®) requires a codified safety protocol, approved by the CSO, before the acquisition of drill Simunition® or associated equipment. Regularly scheduled drills, requiring written approval, can be approved in advance if an exercise plan is developed and briefed along with job hazard analyses. See RM D&S SLE 04-03 *Protection Services*, for additional requirements.

(3) The exercises and drills will be reported by the AOSC in the area office's annual security report with lessons learned and recommended improvements.

15. **LE Response.** RSAs, as defined in the current interagency agreement, will provide coordination/liaison assistance for LE response, including annual site orientations and participation in exercises/drills, at mission sites that meet the following criteria:

A. the facility does not have an on-site response force and must rely on local LE for initial response, and

B. the facility does not have a formal process implementing annual orientations and periodic exercise participation for LE.

16. **Definitions.** Refer to 444 DM 1 for additional security definitions.

A. **Critical Components.** An item that has a single point of failure and whose malfunction or absence would be severely detrimental to the overall operation of the electronic security system, or a device(s) that protects critical assets and areas and whose malfunction or absence would impair the capability of the system to deter, detect, delay, or deny an unauthorized individual.

B. **Critical Infrastructure.** The Critical Infrastructure Protection Act of 2001 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Department of the Interior (DOI) and others use the term "key" for "critical." The below definitions were generated or adopted by the Reclamation security program to define the various criticality designations of our mission sites:

(1) **M4** (FSL 4 mission site) or National Critical Infrastructure. NCIs are Reclamation facilities so vital to the United States that the incapacity or destruction of such facilities would have a debilitating impact on security,

national economic security, national public health or safety, or any combination of those matters.

(2) **M3** (formerly Major Mission Critical). Mission facilities generally characterized by large, multi-purpose features and high downstream hazards, which are so vital to a specific region of the United States that the incapacity or destruction of such facilities would have a debilitating impact on security, regional economic security, regional public health or safety, or any combination of those matters.

(3) **M2** (formerly Mission Critical). Mission facilities generally characterized by moderately large, multi-purpose features and moderate downstream hazards, which are so vital to the region that the incapacity or destruction of such systems and assets would have a significant impact on security, regional economic security, regional public health or safety, or any combination of those matters.

(4) **M1** (formerly Project Essential). Mission facilities essential to a specific project and its associated service areas, the incapacity or destruction of which would have a significant impact on security, economic security, public health or safety, or any combination of those matters in the associated service areas.

(5) **Low Risk**. (also known as "Very Low Risk" in 444 DM 1) LRs are mission assets whose incapacity or destruction would not likely cause loss of life and have little to no impact on security, local economic security, public health or safety, or any combination of those matters. Some exemptions for LRs are included in this policy (note that a reference to FSL 1-4 facilities excludes LRs). Non-mission assets that have occupancy but do not fit under the "Occupied" definition are also considered to be LRs. LRs may also be exempted by DOI and the bureau/office head from certain security risk management processes due to economic and resource constraints.

C. **Master Security Inventory.** A list of the occupied buildings, dams, and facilities included within the Reclamation security program. This inventory is maintained by the security office and available from the RSOs.

D. **Mission Site.** Dam sites that Reclamation designated as NCI, Major Mission Critical, Mission Critical, or Project Essential in past SLE 03-02 versions. These criticality designations are now replaced with an FSL designation. (In the security program's internal management, FSL mission sites will be termed as "M" instead of saying "FSL mission sites" (e.g., FSL 3 mission sites become M3s, FSL 2 mission sites become M2s, and FSL 1 mission sites become M1s. LR sites remain LR).)

E. **NERC - North American Electric Reliability Corporation**. NERC is certified as the Electric Reliability Organization by Federal Electric Reliability Commission as required by the 2005 Energy Policy Act. Reclamation is a NERC Registered Entity due to generation and facilities that are part of the BES

(1) BES - Bulk Electric System -- Transmission Elements operated at 100kV or higher. Generating resources identified as Black start Resources in the Transmission Operator's restoration plan. Generating resource(s) connected at a voltage of 100 kV or above with:

(d) Gross individual nameplate rating greater than 20 MVA. Or,

(e) Gross plant/facility aggregate nameplate rating greater than 75 MVA.

(2) BCA - BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.

(3) BCS - BES Cyber System - One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

(4) CIP - Critical Infrastructure Protection was approved by FERC Order No. 706 in 2008 and requires Cyber Security protection of BES Cyber Systems.

(5) CIP Senior Manager - Designated as Senior Advisor, Hydropower. A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.

(6) PACS - Physical Access Control Systems is the NERC terminology and acronym for EACSS.

(7) PSP - NERC defined term for the physical border (walls, barriers, etc.) surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

F. **Occupied Structure.** Buildings or structures occupied by DOI employees at least 50% of the time, where 50% occupancy is based on an average 40-hour week (e.g., 20 hours per week per 12-month period or 40 hours per week for at least 24 weeks or 1,040 hours per 12-month period). Non-mission assets that have occupancy, but do not fit under the "Occupied" definition, are LRs.

G. **Security Equipment.** Any electronic or physical equipment, device, or component in place to support the security mission at the asset or site. This includes security system detection equipment, access control devices, alarm communication and display components, closed circuit television cameras, monitoring devices, digital/network video recorders, automated access control card readers, intrusion alarms and related components (e.g., servers, circuit boards, conveyance junction boxes), and physical

devices (e.g., fencing, gates, doors, locks). "Critical" equipment include any detection, access control, and surveillance devices that if damaged, destroyed, or otherwise compromised would: undermine a substantial or critical portion of the system; have a significant effect on the sites ability to perform its mission; or require the implementation of compensatory measures.

H. **Security Measure.** Equipment, procedures, or measures designed to deter, detect, delay, or deny unauthorized attempts to gain access to an otherwise restricted or secure area, including guards. Security measures also include protocols associated with these capabilities, such as use of a personal identity verification card for access to the facility.

I. **Security System.** A collection of security equipment and measures intended for any of the following purposes:

(1) Control of access to a Reclamation facility or critical project asset (may include equipment controlling circulation of personnel within a facility),

(2) Delay, detection, deterrence, or assessment of unauthorized access to, or misuse of, Reclamation facilities or critical project assets,

(3) Mitigate, or respond to, risk from attack on Reclamation facilities, employees, or visitors, or

(4) Monitor, assess, or report any of the above.

J. **Transferred Works.** Facilities owned by Reclamation but operated and maintained by an irrigation district or other entity.

17. **Review Period.** The originating office will review this release every 2 years.

RECLAMATION
Managing Water in the West

# RECLAMATION MANUAL TRANSMITTAL SHEET

Effective Date: **09/03/2020** Release No. **655**

Ensure all employees needing this information are provided a copy of this release.

## Reclamation Manual Release Number and Subject

**SLE 03-02 Facility Security**

## Summary of Changes

**Major Revisions throughout document including: aligning better with DHS and DOI requirements such as by aligning assessment schedules and redefining security criticality designations; removing redundancies between this and other DOI or Reclamation policies; Clarification of previously questioned requirements; melding responsibilities with requirements; and reformatting to match new D&S requirements.**

NOTE: This Reclamation Manual release applies to all Reclamation employees. When an exclusive bargaining unit exists, changes to this release may be subject to the provisions of collective bargaining agreements.

## Filing instructions

| Remove Sheets | Insert Sheets |
|---|---|
| **SLE 03-02 pp 1-28** | **SLE 03-02 pp 1-27** |

All Reclamation Manual releases are available at http://www.usbr.gov/recman/

Filed by: **Katherine Wheeler** Date: **09/11/2020**