Reclamation Manual

Directives and Standards

Subject: Facility Security

Purpose: To establish facility security program requirements for the Bureau of Reclamation (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); Code of Federal Regulations (CFR) Chapter 43 Part 422 Law Enforcement Authority (43 CFR 422); 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, Mission Assurance and Protection Organization (MAPO)

Contact: MAPO, Security Division (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 17.G) facilities and structures, except as defined in paragraph 2.C. Transferred Works 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 Part 444, Chapter 1, *Physical Security Program Requirements* (444 DM 1) and paragraph 17.B.5), except where specified, or where security measures are 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 (e.g., special agent and security guard management, intelligence support, and law enforcement (LE) support). The CSO will coordinate with other risk management offices to develop and implement security policy and processes (e.g., emergency management, dam safety, and facility operations).

      (2) Regional directors (RDs) 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, Department of the Interior (Department), 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 will have a qualified, full-time regional security officer (RSO) 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, security awareness, mission facility response, and criminal investigations. RSAs will keep regional and Security Division management informed of these coordination's, resulting information, and provide pertinent advice and counsel.

      (3) An area office security coordinator (AOSC) will coordinate and oversee security functions and training, as well as provide support to the area manager, RSO, RD, and the Security Division 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 as a duty assigned to more than one employee.

(4) Each National Critical Infrastructure (NCI) facility will have an experienced, full-time, on-site facility security manager trained per Departmental and Reclamation requirements and 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 SLE P01, *Security Program,* and 444 DM, Chapter 1, *General Program and Physical Security Requirements* (444 DM 1), must be dedicated to the security function and must be on site for a majority of the work week. 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 their area office.

4. **Training Requirements.**

A. **Security Awareness Training**. The AOSC, RSO, or Security Division will provide annual security awareness training to all Reclamation employees as indicated below. New employees must complete this training within 60 days of initial employment.

(1) The Security Division's information security program manager will maintain and provide annual Reclamation-wide security awareness training to keep all employees compliant with Federal requirements, such as from the Interagency Security Committee (ISC) or the Department.

(2) RSOs, in coordination with the RSA and AOSC, will develop and provide additional training specific to their region, area, and facility to address roles and responsibilities (in relation to the implementation of security program requirements and threat response measures), protocol for observation and reporting of incidents and suspicious activities, unique facility nuances such as site-specific operational security requirements and issues, tourism security needs, or expectations to support local security or LE emergencies. The RSO and AOSC must review materials annually, at minimum, and update materials as circumstances require.

(3) Except for onboarding training and the annual security awareness training provided by the Security Division, the AOSC must document all completed security training and include topics covered, date, time, names of attendees, and the trainer. The AOSC must make this documentation available to the RSO or Security Division upon request.

(4) The AOSC must report all completed security training 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, comprising 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 Division 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.** 444 DM prescribes security standards that facilities must apply 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 training, 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 applies to all mission facilities and occupied Reclamation assets with an 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 contained in DM Parts 441-446 for more security program requirements. In regard to the Reclamation security program, 444 DM supersedes 753 DM until it is updated and has been approved for use by the Department.

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. Reclamation's default protection level is the same as DHS' National Terrorism Advisory System. Reclamation will utilize DHS Dams Sector Protective Measures Handbook—Appendix A, which lists recommended protective measures at each National Terrorism Advisory System 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. The AOSC and the coordinating staff will only include the response measures planned for usage 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 and Security Division will be notified by the area office whenever there is a change in risk or when implementing additional response measures.

C. **Federal Information Processing Standards-200.** Facility and area managers will ensure qualified personnel design, procure, install, and operate all electronic security systems 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, is physically connected to the local EACSS network, is assigned a unique IP address, and has 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 also 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 12977 which currently includes:

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

(b) *Items Prohibited in 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) *Guard Requirements*, facility and area managers will apply the ISC's *Armed Contract Security Officers in Federal Facilities: An Interagency Security Committee Best Practice* 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 standards contain minimum requirements for the protection of BES cyber systems. CIP-014 identified Reclamation-owned transmission substations and stations as well as the primary control center, having operation control, have specific local requirements for threat analysis and security plan details more specific than federal and DHS criteria. Facility and area managers will ensure all security systems used to protect all impact-rated BES cyber systems and transmission substations and stations, identified under NERC-CIP, are compliant with applicable Reclamation NERC-CIP requirements.

6. **Security Criticality Designations.**

A. 444 DM 1 requires an FSL designation 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 (i.e., NCI-LR), used by Reclamation to characterize the relative criticality of all Reclamation dam facilities. The area or facility manager will determine whether to maintain former LR designations per the allowed exemption, or to adopt the new FSL 1-4 designations for mission sites. FSL designations for mission sites are also called M1-4 (further defined in paragraphs 17B and E.).

(1) 444 DM 1.8 B *Facility Categories* designates NCIs as FSL 4 but also maintains their NCI designation. The Department maintains the current list of NCIs.

(2) The region or Security Division must make any future change in FSL or LR designation through a formal decision document (per paragraph 8) which must include a recommendation for 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 decision document must detail a breakdown of the assets and their differing designations (per paragraph 8). To ensure inclusion within security program processes (i.e., risk assessments), Reclamation-owned assets outside of the facility's footprint, but critical to the mission of the facility (e.g., communications equipment), 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. At least every 5 years, the RSO must review and update the master security inventory to ensure all mission-critical assets and all occupied assets are included and have the

correct criticality designation. Any changes must be reported to the Security Division for updating the master security inventory database.

D. The Security Division will maintain the master security inventory that includes FSL criticality designations.

7. **Security Assessments.** The Security Division 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 Security Assessments for Departmental assessment requirements and paragraph 8 of this D&S 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 FSL 3: Every 3 years 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 and NCIs	ISC-RMP FSA	Every 3 years
	FSL 1-4	Internal Control Reviews	Annually (also, as needed, in support of oversight and program management)

[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 RSO will accomplish the ISC-RMP process per 444 DM 1. For added mission facilities or assets, regardless of FSL, the Security Division 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 30 for the assessment to be documented as an accomplishment in current fiscal year annual reporting.

	Facility Applicability	Assessment Type	Minimum Required Frequency
	All sites with Guards	Guard Effectiveness Assessment	FSL 3-4: Every 3 years 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 evaluates potential risks to the public and Reclamation staff and facilities resulting from unauthorized activity by malicious or criminal actors. The CSR analyzes 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 Security Division uses the resulting assessment and risk analysis to identify appropriate risk-reducing actions and provides a relative priority for funding mitigation activities. Frequency requirements are indicated in the previous table.

(1) The CSO, or designee, is responsible for ensuring a CSR team lead is assigned for each review. Each CSR team will include a physical security specialist, facility representative, AOSC (or area office designee), and RSO (or a team lead approved designee). The CSR Team will determine appropriate additional personnel from the Security Division, regional office, area office, and facility (including transferred works personnel) for the CSR team.

(2) The Security Division will schedule CSRs to meet review requirements. The RSO will conduct a PSR as a preparatory step for the CSR site visit. The site visit should serve as an opportunity to verify the PSR. The final signed PSR is due within two weeks of 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) The CSR team lead will complete a formal risk analysis for mission assets using the security risk analysis template (located on the Security Division SharePoint site). The CSR team lead will complete this analysis no later than 30 days after the site visit.

(7) RSAs, as defined in the current interagency agreement, will provide the Security Division with an understanding of LE response capabilities (e.g., 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 providing it to the Security Division's IST for integration into the formal threat assessment report. If the RSA is unavailable, the Special Agent in Charge will ensure these tasks are accomplished by another RSA from a neighboring region.

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

(9) The CSR team lead will document any CSR findings, including any recommended mitigation actions in a report. 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, the CSR team will brief leadership on the assessment's observations and recommendations. If any items identified warrant additional discussion or resolution, the Security Division may 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 CSR report will document any recommended decisions made by the SAT and will 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 evaluates 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 does not address significant issues or make formal recommendations. However, the decision document must include any issues requiring funding (per paragraph 8).

(1) The RSO is responsible for ensuring the accomplishment of all scheduled PSRs each year. The previous table includes the frequency requirements.

(2) In years when qualified personnel conduct a CSR, the RSO will complete the PSR 2 weeks after the CSR site visit.

(3) The Security Division, in coordination with the RSO, will establish and maintain the annual PSR schedule.

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

(5) The RSO must document PSRs using the most recent template available from the Security Division. The RSO will ensure all PSRs are signed, and subsequently posted on the Security SharePoint site, by September 30 of the current fiscal year.

(6) If it is determined that a more detailed risk assessment is needed, the RSO must notify the CSO, area manager, and AOSC via email before the PSR is finalized.

D. **Annual Security Equipment Inspection.** The AOSC will annually account for and inspect all security equipment to ensure it is operating properly. The ASEI, typically conducted by the AOSC, is an oversight function that others can accomplish as directed. The inspection lead will document the ASEI and provide the inspection 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 AOSC must report the date and findings of the ASEI, as well as any corrective actions, in the area office's annual security report. The AOSC must ensure the ASEIs are accurate with periodic oversight by the RSO. The RSO must ensure ASEIs are completed annually before the fiscal year end.

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 Department requires the ISC-RMP for facilities, dams, and other mission structures (e.g., power plants and control centers) occupied by Reclamation employees as defined in paragraph 17.G.

(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 will ensure 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 division. Multi-tenant facilities do not need to use the Reclamation template.

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

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

(1) Each program lead will conduct at least one annual internal control review. The program lead will document the internal control reviews which must include:

(a) name and title of reviewer,

(b) date of review,

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

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

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

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

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

G. **Security Issue Evaluation.** An SIE evaluates a specific security issue and the potential mitigation alternatives. Typically, a security assessment identifies issues requiring an SIE. Risk factor surveys, security-related incidents, exercises, general research, or proposed changes to previous decisions or security posture may also trigger an SIE. The RSO will maintain communications with the facility and area office to properly

submit any identified issues 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 project team leader will establish a SIE project team 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) An SIE decision document will be prepared by the team conducting the evaluation and submitted to the Security Division 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.** An 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 decision document must initiate an SCAS (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. The Security Division then uses this rating to prioritize Reclamation-wide mitigation activities and to provide a relative quantification of risk to aid decision makers in determining if mitigation actions warrant a specific asset. The Security Division staff, in collaboration with regional and area office staff, conduct, review, and update the risk analysis prior to CSRs, SIEs, SCASs, or as changes occur that might affect the risk rating of a facility. The AOSC and RSO will notify the Security Division of any changes in risk. The Security Division will update the risk analysis after significant mitigation activities have been completed at a facility. The CSR team lead will complete a formal risk analysis will be 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 support risk assessments (see paragraph 7.B) or respond to critical intelligence indicators or management concerns. The IST 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. The responsible RSA, as defined in the current interagency agreement, or RSO, will collect the local threat assessment information and provide this information to the IST for integration into the final threat assessment.

(3) **Technical Visits.** Site visit requests (i.e., technical site surveys or site assistance visits) that require members of the Security Division staff, must be approved by the CSO. The team lead will document these visits in a trip report and distribute to the facility, Security Division, and other management based on the purpose and findings.

(4) **Program Integration and Management Activities.** The RSO and area office must conduct periodic collaborative activities to ensure security processes are 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 informational 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 effectively integrated security is into normal processes and programs.

J. **Recommendation Tracking.** The Security Division staff will maintain a database that tracks all risk assessment recommendations. The Security Division will send a recommendation tracking report 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 Division 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, area manager, and RSO.

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

A. **Decision Document.** Any Reclamation employee may recommend a security decision document to the RSO. The decision document 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 beyond or in deviation of the minimum-security standards for that asset (see paragraph 10.A). If there is a decision warranting action that requires funding from the Security Division, the decision document will describe the recommended mitigation action, supporting justification, timeframes, estimated cost, funding sources, and responsible office for implementing that recommendation. If a decision is made to take no action, then the decision document will include 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. Decision documents are not needed for funding requests to bring a facility into compliance with the Security Division's Minimum Physical Security Standards (further defined in paragraph 17.D).

B. **Concurrence Levels.** The CSO is delegated the authorities contained in 441-444 DM and paragraph 4 of the RM Delegations of Authority release. Security decision documents require signatory concurrence at the following levels. Electronic signatures are acceptable.

	Mission Sites	Area Manager[1]	Regional Director[1]	Chief Security Officer[1]	MAPO 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
[4] "Other" includes decision documents (e.g., decision memorandum). PSRs are not considered decision documents.

9. **Consultation with Project Beneficiaries.**

A. The regional or area office responsible for the facility must accomplish all security-related consultation requirements of Public Law 110-229, Section 513. The RSO, with the assistance of the Security Division, 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. The project beneficiary assumes the costs for consultation.

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 Requirements.**

A. **Compliance.**

(1) The minimum required security measures for a mission asset are determined by the Minimum Physical Security Standards (further defined in paragraph 17.D) managed by the Security Division. The area and facility managers are responsible for appropriately implementing, using, and maintaining mission assets.

(2) Minimum Physical Security Standards are based on the ISC FSL standards per 444 DM 1 and are only applicable to unoccupied mission assets. The document listing these standards is available via the Security Division or Security SharePoint site. This document also includes the deviations for all FSL measures not included as minimum standards for Reclamation's mission sites.

(3) Per paragraph 6.B, a facility's designation applies to all critical mission assets at that facility. The standards for that designation level must therefore apply to all the mission assets for that facility, per the latest criticality asset list managed by the Security Division, unless otherwise approved per 10.A.(5) below.

(4) The facility manager, AOSC, and RSO are responsible for gaining compliance at all M1-4 sites. The AOSC, with the assistance and oversight of the RSO, will track the progress of all activities to gain compliance using the latest compliance document (Minimum Physical Security Standards) template provided by the Security Division.

(5) In cases where an asset is unable to implement or maintain a required measure, the AOSC will work with the facility manager to submit a justification for the deviation (this template is available via the RSO or Security Division) for documented approval by the area manager, RSO, and CSO.

(6) As part of the PSR process, the RSO will review update, sign, and subsequently post a compliance document for each facility to the Security SharePoint site.

(7) The Security Division will conduct oversight or periodic checks of this compliance process.

B. **Design of Security Systems.**

(1) **Consistency with Decision Documents.** The area and facility managers are responsible for ensuring all security system designs and equipment are commensurate with the Reclamation minimum physical security standards, and any 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). Reclamation will not install new security systems

or equipment, or significantly upgrade or modify existing systems, without an approved decision document as described in paragraph 8. At Transferred Works, security equipment and systems will be consistent with security requirements and the security strategies and mitigation measures established in Reclamation's security risk assessments of the facility.

(2) **Integrated Design.** All employees, including the area and facility manager, will integrate physical and technical security measures and systems, 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 Division. 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 are 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 hazard dam, or other critical mission asset, the area and facility manager will consult with the RSO during the initial planning and design phase for security concerns and will review the designs 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 Division, must be reviewed and approved via email by the Security Division's lead physical security specialist before initiating the procurement process. Reclamation highly encourages all security system designs, regardless of funding, be reviewed by the Security Division. Reviews will help ensure the intent of the recommendation is met; components are compatible; there is a positive track record for reliability, maintenance, and ease of operation; there is compliance with applicable industry, Federal, Departmental, and Reclamation physical security standards and information technology (IT) compliance requirements; and the approval adheres to cost-effective procurement and O&M strategies.

C. **System Components**.

(1) Area and facility managers must consult with MAPO physical security specialists 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 MAPO 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) Area offices and facilities must purchase all security system devices in accordance with Executive Order 13873 - *Securing the Information and Communications Technology and Services Supply Chain* which prevents the purchase of information technology equipment from nations which are adversarial to the United States. Security system device purchases will 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 program and obtain the necessary IT approvals prior to purchase.

(3) Area offices and facilities must also purchase all security system devices 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.

D. **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) The facility's current or planned equipment maximizes security effectiveness, including proper monitoring and prompt assessment and response.

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

(3) The NCI-SM or designee must review all security system alarm and error logs, or automated reports generated by the security system 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 correct the issue(s). The NCI-SM or designee must review these logs or reports regularly in accordance with documented policies and procedures. The NCI-SM will document, investigate, and correct all system issues and anomalies in the facility's normal O&M management system in a timely manner to prevent any increases in security risks.

(4) The facility manager must document and include a summary of significant outages, failures, and corrective actions as they occur in the area office annual security report (see paragraph 13.B).

(5) The facility manager or designee must maintain as-built security drawings 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 (i.e., alarm controller panels and communications equipment) to complete ASEIs and performance testing on all security equipment. Non-critical, consumable, and easy to procure, low-cost commercial-off-the-shelf equipment (less than $5,000) do not need to be inventoried. Examples of low-cost commercial-off-the-shelf equipment include surge suppressors, fuses, and power supplies.

E. **Maintenance of Security Systems.** The facility manager or designee is responsible for properly maintaining, testing, repairing, and replacing all security systems and equipment, as needed, to maintain the security mission of the facility. 444 DM 1 includes additional requirements for security equipment maintenance. The facility manager or designee may contact the Security Division for additional guidance on maintenance and replacement of security equipment and associated frequencies. The facility manager will ensure:

(1) all security equipment and programs are maintained and 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) the NCI-SM or designee conducts performance testing of security equipment to ensure functionality and effectiveness. The NCI-SM or designee will test all security equipment annually per 444 DM 1. The performance tests will be performed using the Reclamation Power Equipment Bulletin 59 and individual component technical orders or manufacturer specifications. The NCI-SM or designee will document and route performance testing through the facility manager and the area office's O&M position in charge of facility maintenance for concurrence. The area office's annual security report will detail any significant findings.

(3) the facility manager or designee conducts annual preventive maintenance inspection/procedures on all security equipment to ensure all are operating nominally and within manufacture specifications (see Power Equipment Bulletin 59 for additional guidance). The preventive maintenance inspection/procedures will be documented and routed through the person in charge of facility O&M and the AOSC for concurrence. The area office's annual security report will detail any significant findings.

(4) equipment malfunctions or outages are immediately reported to facility maintenance staff or entered into the maintenance tracking systems following facility procedures. If failure of any security system critical component(s) at an FSL 3-4 creates a significant vulnerability to mission assets or personnel (i.e., loss of multiple sensor components at one facility), the facility must notify the area manager immediately and the RSO within 24 hours. Reporting for equipment issues at an FSL 1-2 is at the discretion of the area manager. The facility manager must implement compensatory measures (i.e., measures that ensure equivalent security capabilities without any increase in risk) immediately for all security mission critical equipment (see paragraph 17.H) or within 5 days for all other equipment. Per 444 DM 1, if interim measures are not implemented then the deviation must be documented, retained, and immediately submitted to the RSO. The compensatory measures must be maintained until the equipment is back in full service. The area manager will brief the RSO 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 needs are regularly sent to the RSO and the Security Division to accommodate major upgrades or replacements for security systems or components that have exceeded their end of useful service life (see paragraph 10.E.(8) and RM D&S SLE 05-01, *Reimbursability of Security Costs* (SLE 05-01)). 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 will 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, qualified personnel must replace IT components prior to becoming end-of-life when the vendor stops supporting the equipment, regardless of site criticality level, operational status, or system type.

(c) Non-perishable items that have reached the end of their useful service life and are still in serviceable condition will remain in service. The facility manager will inspect all equipment 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 risks, preventative maintenance reports, recommendation of facility manager, or reviews performed by the RSO or Security Division.

(d) The facility manager will replace perishable technologies at the end of their useful service life, regardless of site criticality level, operational status, or system type. Perishable technologies include, but are not 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 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., prohibited items, 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 Division.

12. **Funding.** The facility security program uses funds from Reclamation's Site Security Fund and a portion of this fund (A5) is set aside annually for non-reimbursable security fortifications. The facility security program will use A5 fund for security fortification costs at critical water and power facilities (FSL 1-4 mission sites) only. The region, area, or facility funds needs identified at non-mission critical or occupied facilities using an applicable appropriation as defined in other policies or rules. Additional funding information including definitions for terms used in this paragraph (such as fortification, end of useful life (also called service life), and replacement) are within SLE 05-01.

    A. **Responsibilities.** The Chief Security Officer, RDs, and area and facility managers are responsible for ensuring the appropriate usage of Reclamation's Site Security Fund. The security division's budget lead and budget analyst, RSOs, and the budget leads at regional, area, and facility levels for security projects are responsible for the daily operations and management of the accounts set up within the fund. The RSO and the regional budget analysts are responsible for ensuring security accounts are not mis-used or charged to without prior approval from the security division budget lead.

    B. **Funding Requests.** The RSO will submit requests for usage of the A5 fund that include the funding request, regional priority, and amount for approval by the Security Division's Facility Security program manager and budget lead. The budget lead will determine if funding is available, and the Facility Security program manager will determine the programmatic priority at which the request will be funded.

    C. **Usage of the A5 fund.** Typical uses of the A5 fund are summarized below.

        (1) Formal Recommendations and minimum physical security standards. Approved formal recommendations and requests for minimum security standards, per paragraph 8, may use A5 funds for purchasing, contracting, designing, installing, testing, and training on equipment, materials, and other resources including services. All funding requests made to help a facility gain compliance do not need a decision document, per paragraph 8.A, but the RSO will input a formal recommendation into the security database per normal processes. The RSO will notify the Facility Security program manager and security division budget lead which fiscal year the facility will implement the recommendation and then the budget lead will fund the request according to funding priorities and availability.

        (2) End of Useful Life Equipment. Approved replacements that have reached their end of useful life per paragraph 10.E.(8) may use A5 funds at the discretion of the Security Division. The replacement of equipment during its normal life cycle (see

SLE 05-01, Appendix A) is a standard maintenance cost and is funded from facility O&M. Those requesting usage of the A5 fund will submit their request via email using the latest guideline and template available via the Security Division budget lead. The RSO will make any A5 requests to the Security Division's Facility Security program manager and budget lead who will then fund the request based on priority and amount.

(3) Less than $10,000. Funding requests under $10,000 that do not fit into either via 12.C (1) or (2) may also be approved using the same process outlined in 12.C (2).

(4) No O&M. Facility O&M funds the O&M of equipment and systems, not the Site Security fund. Security-related O&M activities, other than guards and patrols, include all activities related to the operation and maintenance of security at a facility, such as operation and monitoring of security equipment, equipment maintenance, ASEIs, and other equipment inspections and tests. These security-related O&M activities are funded upfront or charged to facility O&M funds. RDs and area and facility managers must budget for these security-related O&M activities.

(5) Guards. Facilities may use A5 funds for exigent circumstances or for new guard capabilities including standing up a new force at an NCI or buying equipment and materials for a new defense capability. Increased levels of guards and patrols, and replaced or upgraded guard equipment, is not authorized for purchase under A5, per Public Law 110-229 Section 513 (b) (1), until the fiscal year's reimbursability ceiling amount has been exceeded.

13. **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 Division for revision in risk analysis numbers, security measures, or overall risk management strategies.

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

(4) RDs must keep the CSO 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. **Regional and Area Office Annual Security Report.** The AO and RSO will submit an annual report to the Security Division addressing the requirements outlined in 444 DM 1.6.D.(3) and 1.9 C *Annual Reporting* as well as any additional information contained in the annual report template provided by the Security Division. The Security Division will provide the overall programmatic summary report to OLES.

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.** The area office, in collaboration with the RSO and the facility, must develop an SSP for all unoccupied FSL 1-4 mission facilities. 444 DM 1 defines SSPs and specific plan components. The area office must coordinate with Transferred Works to develop and maintain effective SSPs for each facility.

(1) The area office must use the SSP in conjunction, and avoid contradictions with, Standing Operating Procedures (SOP) and the Emergency Action Plans (EAP). The area office may integrate the SSP 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.

(3) SSP templates and checklists are available on the Security SharePoint site or from the RSO. SSPs must address all components within the template including, but not limited to, the signature and revision pages. The RSO must initially review any SSPs to ensure completeness and accuracy. The area office will upload a copy of the signed SSP and any revisions to the Security SharePoint site.

(4) The area office will ensure the SSP is used for real world events (including construction or other events that could potentially increase risks) and for developing security program objectives, injects, exercises, drills, and tests. The area office will update the SSP to reflect lessons learned from any real world or exercise events, as appropriate.

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 notify public safety agencies downstream of the dam and response actions to intervene at the dam site. Refer to RM D&S EMG 03-01 *Serious Incident Reporting and Duty Officer Program,* for reporting guidance and FAC 01-01 for EAP requirements. 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.

(5) The AOSC must coordinate with the area office EAP coordinator to ensure a facility's EAP integrates the notification contact list for security and response personnel.

(6) The AOSC and RSO must collaborate with the EAP coordinator to determine an opportunity or need to include security components/scenarios for all FSL 3-4 sites. This includes participating in the planning and conducting exercises to provide collaborative integration of security response activities, as deemed appropriate by the area manager.

(a) The RSO will document and communicate any security-related information and recommendations resulting from the exercise with the Security Division.

(b) The RSO will implement and track security recommendations and complete any SSP and security program updates.

14. **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 sticker or other means of identification, and be escorted at all times. The AOSC/NCI-SM 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* contain tour and visitor center security information. Facilities must consider these guidelines when designing or changing public tours and visitor centers to integrate security designs, procedures, and best practices and to ensure the safety and security of visitors, employees, and facilities.

B. **Establishing and Conducting Public Tours.** Public tours (see definition, para 17.K.) at Reclamation facilities can potentially increase security and safety risks. To ensure the security and safety of employees, the public, and our facilities, the following steps and requirements must be followed in establishing and maintaining a public tour at Reclamation facilities.

(1) Determination of the tour route.

(a) Tours must not be taken into areas where photos or videos are not permitted, including any restricted areas such as operations/control/monitoring rooms, IT/SCADA spaces, or other high-risk assets or asset components.

(b) Area offices will establish an evaluation team comprised of the RSO, a Security Division staff member, a facility manager, an Occupant Emergency Plan (OEP) representative, and a safety representative to establish a safe and secure tour route.

(c) The tour must include the following security measures when accessing and along the tour route where appropriate, or else provide a documented deviation justification.

(i) Install signage in parking lots and areas leading up to the tour route to notify visitors that no purses, bags, or similar hand-carried items will be allowed on the tour.

(ii) Inform tour route visitors of the restrictions in place, such as staying aware of surroundings and each other, information security rules, physical security rules, what they can and can't bring, etc.

(iii) Escort all visitors along the tour route.

(iv) Conduct a check after each tour to ensure all critical asset nodes are secure (e.g., no unauthorized access, tampering, IEDs, or other potential sabotage have occurred).

(v) FSL 3 and 4 facilities also must:

(aa) install access-controlled doors and barriers between the public and the assets of concern,

(bb) install cameras with smart analytics to detect and assess visitors leaving tour zones or staying too long in any access areas, and

(cc) conduct visitor screening (via x-ray, magnetometer, etc.).

(d) The team will document:

(i) facility/site name,

(ii) purpose of the decision document with an approximate tour commencement date,

(iii) proposed route with diagrams, a list of personnel/offices, mission assets and anything else potentially affected by the route or presence of the public onsite,

(iv) a description of the tour route itself starting with the visitor parking area, all access points, locations the tour will stop, where the tour will end, the potential routes visitors will access to get back to the parking lot, etc., as well as the existing security measures in place along the route and access points,

(v) risk factors such as proximity to any restricted/sensitive areas per B. (1) above, direct or indirect, including the risks of casual exposure to sensitive areas, documents, or other media such as those which may be found on desks, walls, platforms, etc.,

(vi) evaluation findings, conclusions, and mitigation recommendations that include each security measure listed in B.(1)(c) above, as well as how it is being met, should be met, or won't be met (with a deviation justification),

(vii) proposed modifications to the OEP to account for the visitors being anywhere along the route, the applicable safety plan(s) to account for the visitors being anywhere along the route, and to the SSP for any mission assets potentially affected by the route or presence of the public onsite, and

(viii) estimated costs and timeframe for site preparations for the tour, such as buying and installing electronic security and access control equipment, video surveillance, screening equipment, signage, etc.; any OEP or safety modifications; and all document revisions and approval processes.

(2) Approval and Implementation

(a) Once the team has completed and documented their route evaluation, they will brief and provide the document from B.(1)(d) above to the area manager for review and a determination whether to proceed with the formal decision document process as outlined in paragraph 8 of this D&S.

(b) Upon approval, the area office, in consultation with the RSO, can proceed with the next steps in establishing the tour with site preparations, documentation, and training.

(c) Collectively, the RSO, AOSC, and facility manager are responsible for ensuring all previously identified security and safety measures or mitigations

are approved and properly planned per paragraph 8, funded (if necessary), implemented (consultation with the Security Division is strongly advised), and maintained. Significant security-related changes or deviations from the original approved decision document must be submitted to and reviewed by the Security Division to determine whether a new decision document should be accomplished.

(d) Increased physical security measures required due to the addition of public tours may be eligible for the Security Division fortification funding; however, the facility shall fund all the necessary guards and associated security reimbursable ceiling impacts.

(e) The AOSC, RSO, and facility manager will update/amend the facility's SSP, EAP, and OEP to reflect the security, safety, and training policies, procedures, and any mitigation measures required.

(f) The RSO must review and approve the amended SSP and forward the updated signed version to the Security Division.

(g) The area office is responsible for providing all tour guides and visitor center personnel with initial and biennial security awareness and tourism security training. This training will be documented and must include the participant's name, their position (tour guide, visitor center staff, etc.), the name of the person providing the training, and the date, time, and location of the training.

(3) Validation.

(a) Once all items in (2) above have been accomplished, the AOSC will request the RSO conduct a site visit to validate the completed requirements. Site tours will not be conducted until validation has been completed and all requirements have been met. RSOs will use the information obtained in B.(1)(d) above as the basis for their requirements validation and attach a copy of the tour route evaluation with their validation memo/document.

(b) Upon validation that all requirements have been satisfactorily accomplished, the RSO will prepare a short memorandum (or email) to the area manager along with a courtesy copy to the AOSC, CSO, and facility manager, stating all requirements have been accomplished and the facility may now conduct tours. The memorandum (or email) will include the facility's name, the names of the person(s) conducting the validation, the date of the visit, and any other relevant comments or suggestions. A copy of the validation report will also be attached.

(c) In the event the validation process determines that all requirements have not been accomplished, the RSO will prepare a short memorandum (or email) to

the same addressees in (b) above stating the reason(s) validation could not be accomplished. The memo should also include any comments, suggestions, or recommendations that would aid the site in achieving validation. In consultation with the Security Division, the RSO will determine whether a new site visit is required or if validation can be achieved through other means, such as submitting photos that clearly show the requirement has been met. In either situation, whether a new site visit is required or not, the RSO will document the determination and validation status of the facility using the instructions in either this paragraph or (b) above.

(d) The AOSC and facility manager will maintain copy of the most current tour validation in the SSP.

(4) Maintaining Tours.

(a) All changes to public tours with 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.

(b) The area office is responsible for conducting periodic oversight of the tour to ensure it complies with the approved decision document.

C. **Non-public Tours.** Non-public tours (see definition in paragraph 17.K.) must be scheduled with the facility before the tour. Hosting offices will obtain a list of tour participants, determine the tour route and information, and notify the RSO and area office. Non-public tours will not include access to sensitive or restricted areas without verification of "need to know."

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, and Departmental Manual 445 DM 3, *Foreign Visitor Access Management Program*, which requires monitoring foreign visitor access to DOI facilities.

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 directly benefits the facility can be funded if approved by the formal decision process (see paragraph 8).

F. **Photography or other media.** When contractors or visitors are present, the facility manager must ensure written documentation is in place regarding protecting information and operations related to restricted/critical assets or information within the facility. This document must address restrictions on photography, recordings, or other means of information sharing. All processes must be compliant with security-related requirements.

15. **Security Guards.** Refer to the 446 DM series, 444 DM 1.8 D (5) Guard Requirements, and the RM D&S SLE 04 series for additional security guard requirements.

    A. **Changes.** Before any substantial changes to guard force configuration or manning strength are implemented, 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) *Guard Requirements*, 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 Division. Reclamation-wide facility security program standards and example contract language are available from the Security Division.

    D. **Exercises and Drills.** The area manager integrates security guard exercises and drills into the security training program.

        (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 five 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 force without the express, written approval of the CSO. Evaluating the simulated practical application of significant or potentially deadly force (i.e., drills using Simunition®) requires a codified safety protocol approved by the CSO, before acquiring drill Simunition® or associated equipment. The CSO may approve regularly scheduled drills, requiring written approval, in advance if the facility develops and briefs an exercise plan along with job hazard analyses. See RM D&S SLE 04-03, *Protection Services*, for additional requirements.

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

16. **Law Enforcement Services.**

    A. The CSO is the Law Enforcement Administrator or Bureau Director of Law Enforcement for Reclamation as identified in 43 CFR, 422.5, and 43 CFR, 422.9, and

is the delegated official responsible for conferring Reclamation's Federal law enforcement authority to a law enforcement agency who has entered into a contract or agreement to enforce Federal laws and regulations on Reclamation lands, facilities, and waterbodies. As such, all contracts and agreements for law enforcement services, whether for the enforcement of Federal laws or the laws of a state, must be approved by the CSO after review and consultation from the Special Agent in Charge.

B. 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:

(1) the facility does not have an on-site response force and must rely on local LE for initial response, and

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

17. **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 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.” The Department and others use the term “key” for “critical.” The Reclamation Security Division generated or adopted the below definitions 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 the Department 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. The Security Division maintains this inventory and is available from the RSOs.

D. **Minimum Physical Security Standards.** A required set of security measures that Reclamation must appropriately implement, use, and maintain at mission assets depending on their FSL mission designation. These standards are derived and updated from the ISC-RMP standards and maintained by the Security division. The set also includes justifications for deviations, as required by 444 DM 1, for other listed FSL measures.

E. **Mission Site.** Dam sites that Reclamation designates 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 "FSL mission sites" (i.e., FSL 3 mission sites become M3s, FSL 2 mission sites become M2s, and FSL 1 mission sites become M1s. LR sites remain LR)).

F. **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:

(a) gross individual nameplate rating greater than 20 MVA, or

(b) 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, mis-operation, or non-operation, adversely impact one or more facilities, systems, or equipment and would affect the reliable operation of the Bulk Electric System.

(3) 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 – Physical Security Perimeter, 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.

G. **Occupied Structure.** Buildings or structures occupied by Department employees at least 50 percent of the time, where 50 percent occupancy is based on an average 40-hour week (i.e., 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.

H. **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 includes 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.

I. **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. The minimum required security measures for a mission asset are determined by the Minimum Physical Security Standards document managed by the security division.

J. **Security System.** A collection of security equipment and measures intended for 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) mitigation, or response to, risk from an attack on Reclamation facilities, employees, or visitors, or

(4) monitoring, assessing, or reporting any of the above.

K. **Tours – Public and Non-Public**.

(1) **Non-Public Tours.** Tours that are provided to specific groups, organizations, or individuals. These tours are pre-arranged between the facility and the participant organizer. Examples include schools, government officials, visiting dignitaries, etc. Non-public tours will not have access to restricted or sensitive areas without verification of "need-to-know."

(2) **Public Tours.** Tours that are open to the public during specific days and times. Though public tours can include organized groups similar to non-public tours, these tours are generally not scheduled outside the site's pre-established tour hours. Facilities conducting public tours must follow the guidance outlined in paragraph 14 of this D&S. Public tours will not include access to restricted or sensitive areas.

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

18. **Review Period.** The originating office will review this release every two years.

RECLAMATION
Managing Water in the West

RECLAMATION MANUAL TRANSMITTAL SHEET

Effective Date: **10/24/2023**

Release No. **670**

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

Minor revisions to include the following:

•Minor edits for grammar and sentence clarifications.

•Updated procedures and processes in establishing, conducting, and maintaining public and non-public tours.

***Policy and Programs was changed to Mission Assurance and Protection Organization (MAPO) effective 10/22/2023.**

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 1-30	**SLE 03-02 pp 1-35**

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

Filed by: **Maria Clardy**

Date: **10/26/2023**