Reclamation Manual

Directives and Standards

Subject: Facility Security

Purpose: To establish facility security 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 (32 Stat. 388; 43 U.S.C. 391) and acts amendatory thereof and supplementary thereto; Critical Infrastructure Protection Act of 2001 (Public Law 107-56; 115 Stat. 272, 42 USC 5195c); Homeland Security Act of 2002 (Public Law 107-296; 116 Stat. 2135, 6 USC 101); Consolidated Natural Resources Act of 2008, Section 513, Bureau of Reclamation Site Security; Executive Orders 10450, 10577, 12958 as amended, and 12968; Homeland Security Presidential Directives; Federal Information Processing Standard 201 (FIPS-201); and Departmental Manual Part 442, 444 and 446.

Approving Official: Director, Security, Safety, and Law Enforcement (SSLE)

Contact: SSLE, 84-45000

1. **Introduction.** The Facility Security component of Reclamation's Security Program is concerned with the physical, technical, and procedural systems for reducing and managing risks and for protecting Reclamation's employees, contractors, the public, buildings, and physical infrastructure. This D&S prescribes minimum security standards and other security requirements for Reclamation facilities.

2. **Applicability.** This D&S applies to directors and managers responsible for facilities and buildings owned by Reclamation, including those where operation and maintenance have been transferred to an operating entity. For buildings and offices occupied, but not owned, by Reclamation, this D&S must be applied to the greatest extent possible in collaboration with the building owners or managers.

3. **Responsibilities.** Responsibilities are listed in the Reclamation Manual Policy, *Security Program* (SLE P01).

4. **Definitions.** None.

5. **Security Criticality Designations.** The following security criticality designations will be used by Reclamation in the Security Risk Assessment process, application of Reclamation's Threat Condition Protective Measures, and other security activities. Project facilities are placed into each category based on a comprehensive facility prioritization and categorization process. The Chief Security Officer and Regional Security Officers will maintain a list of which facilities are contained in each category.

A. **National Critical Infrastructure (NCI).** Reclamation facilities which are 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.

B. **Major Mission Critical (MMC).** Reclamation 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.

C. **Mission Critical (MC).** Reclamation 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.

D. **Project Essential (PE).** Reclamation facilities that are 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.

E. **Low Risk (LR).** Reclamation facilities where their incapacity or destruction would only have a minor impact on security, local economic security, public health or safety, or any combination of those matters.

6. **Tours, Visitor Centers, and Foreign Visitors.** The following requirements apply to Reclamation tours, visitor centers, and foreign visitors to Reclamation facilities.

A. Reclamation's Visitor Center Guidelines, issued by the Office of Policy and Administration, contains a chapter on Tour and Visitor Center Security. This chapter must be considered when designing or changing public tours and visitor centers. The chapter provides guidelines for integrating security designs, procedures, and best practices into Reclamation tours and visitor centers to ensure the safety and security of visitors, employees, and Reclamation facilities.

B. Tour guides and visitor center personnel must receive initial and biennial training in security awareness and tourism security. This training is the responsibility of the NCI Security Officer or Area Office Security Coordinator.

C. All non-public tours (such as school groups, technical groups, and international groups) must be scheduled with the facility in advance of the tour to allow for vetting of tour participants. The Regional Security Office or Area Office Security Coordinator must also be notified of the tour, as far in advance as possible.

D. The Office of International Affairs in Denver must be notified of all foreign visitors before visitors are allowed to participate on any tour, visit, or activity not normally available to the public. International Affairs will coordinate with SSLE's Information Sharing and Law Enforcement Support Office to ensure each international visitor is properly vetted, and will provide sufficient advance notice to the Regional Security Office or Area Officer Security Coordinator of the planned tour, visit, or activity.

E. All changes to public tours that have a significant security-related impact require an issue evaluation and decision document as described in Section 10.

7. **Security Measures.** Reclamation will implement and maintain physical security measures as determined by Departmental Manual (DM) Minimum Security Standards, security-related decision documents, Reclamation's Threat Condition Protective Measures, appropriate security-related procedures, and other applicable Federal standards.

A. **DM Minimum Security Standards.** DM Part 444 – Physical Protection and Facility Security, Chapters 1 and 2, prescribe minimum security standards that must be applied at all Department facilities, including buildings, offices, and, where applicable, to dams and related project facilities. Chapter 1 – "General Program Requirements" (444 DM 1) identifies five levels of facilities, and prescribes minimum security standards for Levels 1-4. Chapter 2 – "National Critical Infrastructure and Key Resource Facilities" (444 DM 2) prescribes minimum security standards for Level 5 facilities.

(1) **Project Facilities.** Reclamation's security criticality designations are defined in Section 5. A list of facilities in each category may be obtained from the Chief Security Officer or appropriate Regional Security Officer. Reclamation must apply the procedures of 444 DM 1 for determining the most appropriate level of security for a specific project facility; however, the 444 DM 1 security levels generally correspond to Reclamation's security criticality designations as follows:

Security Level 5 – NCI Facilities
Security Level 4 – MMC Facilities
Security Level 3 – MC Facilities
Security Level 2 – PE Facilities
Security Level 1 – LR facilities

(2) **Buildings, Offices, and Complexes.** Reclamation must apply, to the extent possible, the procedures and requirements of *Facility Security Level Determinations for Federal Facilities – An Interagency Security Committee Standard* for determining the most appropriate level of security for buildings, offices, and building/office complexes. The security level of a building or office is based on factors such as facility mission, the total number of employees working at the facility, volume of public contact, and crime area.

B. **Decision Documents.** Recommendations made during security risk assessments, security issue evaluations, security corrective action studies, and other formal processes determine what security measures are required, including minimum security standards prescribed in the DM. Final approved recommendations are documented in a formal decision document. The processes for security risk assessments, security issue evaluations, and security corrective action studies are described in Sections 9 through 11.

C. **Threat Condition Protective Measures.** Threat Condition Protective Measures are additional security measures that are placed in service based on the Homeland Security Threat Condition system and approved actions from Security Risk Assessments. These measures vary based on the threat condition level and the facility criticality designation. Information regarding Reclamation's Threat Condition Protective Measures can be obtained from the Chief Security Officer or Regional Security Officer.

D. **FIPS-201.** All electronic access control and security systems purchased or deployed by Reclamation after February 19, 2004, must be compliant with the FIPS-201, *Personal Identity Verification of Federal Employees and Contractors*, and related implementing standards and specifications.

8. **Advisory Teams.** Reclamation will utilize review or advisory teams to provide oversight and consistency in the application of security risk management strategies and mitigation activities throughout Reclamation. A security advisory team will review security recommendations from all Comprehensive Security Reviews (CSRs). An advisory team will also review security recommended mitigation alternatives from Security Corrective Action Studies (SCASs), unless a project management team exists and performs this function. An advisory team may optionally be used to review security recommendations from Periodic Security Reviews (PSRs) and Security Issue Evaluations (SIEs). Security advisory teams will consist of a mix of representatives, depending on the scope, significance, and complexity of the issues and recommendations, and include individuals such as the following: a manager or other representative from the regional office, area office, and facility; a physical security engineer; a risk management technical specialist; an issue technical specialist; a Regional Security Officer; and the Reclamation Deputy Security Officer. These advisory teams are further discussed in Sections 9 through 11.

9. **Security Risk Assessments.** Reclamation will maintain a reiterative Security Risk Assessment program for all NCI, MMC, MC, and PE facilities. The Security Risk Assessment program will have three primary components: risk analysis, CSRs, and PSRs.

A. **Risk Analysis.** A security risk analysis will be conducted and maintained by SSLE for all facilities using the latest approved methodology for determining and prioritizing risk within the Security Program. The risk analysis data and ratings will be used to provide a basis for site-specific strategy and recommendation development, budget prioritization, and other program activities. The analysis will be reviewed and updated, in collaboration with appropriate regional and area office staff, prior to CSRs, SIEs,

SCASs, and as changes in site factors occur that might affect the risk rating of a facility.

B. **Comprehensive Security Review (CSR).** A CSR is a review and assessment of potential risks to the public, Reclamation staff, and Reclamation facilities resulting from an attack by human aggressors. The resulting estimation of risks is used to identify appropriate risk-reduction actions and provides a relative priority for mitigation activities. A CSR will occur every 6 years for each NCI, MMC, and MC facility. Accomplishment of this review is the responsibility of the Chief Security Officer and will involve personnel from the Denver office, regional office, and area office, including facility and operating entity personnel as appropriate. CSR findings, including any recommended mitigation actions, will be documented in a CSR Report. Each recommendation will include the projected cost, target completion date, and responsible party. The CSR Report will be reviewed by a security advisory team which will approve or reject each recommendation. The recommended decisions made by the security advisory team will be documented as part of the final CSR Report, which will serve as the official decision document.

C. **Periodic Security Review (PSR).** A PSR is a review and evaluation of the security measures and practices in place at a facility and the effectiveness of these measures with respect to, maintenance, proper operations, and consistency with security procedures in the facility Site Security Plan. The PSR is not intended to produce major risk-based recommendations. A PSR will occur every 6 years for each NCI, MMC, MC, and PE facility. For NCI, MMC, and MC facilities, the PSR will generally occur 3 years after the CSR. Accomplishment of the PSR is the responsibility of the Regional Security Officer. PSR findings, including any recommended mitigation actions, will be documented in a PSR Report, using the approved standard PSR Report template. Each recommendation will include the projected cost, target completion date, and responsible party. The final PSR Report will serve as the decision document.

D. **Out-of-cycle Risk Assessment (ORA).** An ORA is a short-term process for developing risk estimates and risk reduction recommendations related to a current threat scenario for a critical asset. An ORA will be conducted if an issue or event arises that could significantly increase risk at the site and a risk-based decision is needed in a short timeframe. An ORA is generally warranted if an event or emerging threat requires an understanding of the risk before a response can be determined, and the potential change in risk is significant (i.e., change in risk value by an order of magnitude). Recommendations generated by an ORA will follow the CSR decision making and approval process.

E. **Significant Issues.** Significant issues include road restrictions, closures, or openings; major fortification activities; significant cost outlays; or major operational changes, such as significant security guard force modification, major changes in adjacent public and private land use, major local demographic shifts, significant local urbanization, and other influential factors. If the final CSR or PSR Report contains significant issues, a

recommendation will be included in the decision document for a Security Issue Evaluation of those significant issues. Security Issue Evaluations are further discussed in Section 10.

F. **Approval Level.** CSR and PSR decision documents will be approved by the area manager, regional director, and Chief Security Officer. This signatory approval level may be further delegated at the discretion of the approving official, but may not be delegated lower than the facility manager.

G. **NCI and MMC Facilities.** Signatory approval of CSR decision documents for all NCI facilities, and CSR decision documents that contain significant changes for MMC facilities, will also include the Director, SSLE; Deputy Commissioner, Policy, Administration, and Budget (PAB); and Commissioner; with concurrence by the Assistant Secretary for Water and Science. Significant changes include road closures, major fortification activities, major public impact, significant cost outlays, or major operational changes, such as significant guard force modification.

H. **Risk Assessments by External Entities.** Many different entities, including the Department of Homeland Security, State Offices of Homeland Security, National Guard Bureau, U.S. Coast Guard, and local governments have recognized the criticality of Reclamation facilities within their jurisdictions. For these and other reasons, Reclamation continues to receive requests from these governmental or other entities to conduct security assessments. All requests for an external security assessment of a Reclamation facility must be submitted in writing to Reclamation. Requests submitted to a regional or area office must be forwarded to the Regional Security Officer for coordination and approval, with concurrence by the Chief Security Officer.

I. **Additional Guidance.** Detailed guidance and procedures for the Security Risk Assessment Program are contained in the Security Risk Assessment Guideline, which is available from SSLE or any Regional Security Officer.

10. **Security Issue Evaluations.** A Security Issue Evaluation (SIE) is a screening evaluation of an issue and potential alternatives to generate additional risk reduction information, determine what mitigation actions could be taken, and determine whether a more in-depth Security Corrective Action Study (SCAS) is needed. Security Corrective Action Studies are further discussed in Section 11.

A. **Evaluation.** An SIE will be used to evaluate all significant security-related issues. Issues requiring an SIE will usually be identified through a CSR, PSR, or vulnerability study, but may also be triggered by security-related incidents, research, information from other sources, proposed changes to previous recommendations and decisions, and proposed changes in security posture, such as changes in security guard strategies or

significant changes to visitor tours. An issue evaluation may be conducted on a specific facility (e.g., structural mitigation at a specific dam) or a group of facilities (e.g., installation of vehicle barriers at facilities that meet certain criteria).

B. **Decision Document.** An SIE decision document will be prepared by the team conducting the evaluation. At a minimum, the decision document must include a discussion of the alternatives considered, and a recommendation and supporting justification to take no action, conduct a SCAS, or implement specific actions without an SCAS. The evaluation team will determine whether the SIE decision document must be reviewed by a Security Advisory Team, based on the scope, significance, and complexity of the issues.

C. **Approval Level.**

(1) SIE decision documents will be approved by the area manager; regional director; Chief Security Officer; and Director, SSLE. This signatory approval authority may be further delegated, in writing, at the discretion of the approving official, but may not be delegated lower than the facility manager.

(2) **NCI and MMC Facilities.** SIE decision documents for NCI facilities, and SIE decision documents that contain significant changes for MMC facilities, will also be approved by the Deputy Commissioner, PAB and Commissioner, with signatory concurrence by the Assistant Secretary for Water and Science. Significant changes include road closures, major fortification activities, significant cost outlays, or major operational changes, such as significant guard force modification or impact to the public.

11. **Security Corrective Action Studies.** An SCAS is a comprehensive analysis of a security-related issue and mitigation alternatives, including costs and risk reduction recommendations. An SCAS will usually be initiated through an SIE decision document, but may also be formally recommended through any decision process provided sufficient justification. A SCAS will generally be accompanied by public involvement, environmental assessment, and similar activities.

A. **Review.** An initial SCAS decision document will be reviewed by the project management team, if one exists, or an advisory team. The advisory team may make suggestions and request further analysis, or they may instruct the SCAS team to prepare a final decision document.

B. **Decision Document.** Written documentation of each recommended mitigation action, final decision, and supporting justification is required. If a decision is made to take no action on an issue or recommendation, then that decision will be documented with

supporting justification. If there is a decision that an action by Reclamation is justified, then at minimum the documentation will describe the decision, including the actions, timeframes, estimated cost, funding sources, and responsible office.

C. **Approval Level.**

(1) The final decision document for a SCAS will be approved by the area manager; regional director; Chief Security Officer; Director, SSLE; and Deputy Commissioner, PAB.

(2) **NCI and MMC Facilities.** Final signatory approval of all SCAS decision documents related to NCI facilities, and decision documents that contain significant changes for MMC facilities, will also include the Deputy Commissioner, PAB and Commissioner, with concurrence by the Assistant Secretary for Water and Science. Significant changes include road closures, major fortification activities, significant cost outlays, or major operational changes, such as significant guard force modification.

12. **Summary of Signatory Approval Levels.** As described in Sections 9 through 11, signatory approval levels vary depending on the type of review and issue significance. The following table summarizes security decision document signatory approval levels.

Decision Document	**Signatory Approval**
Security Risk Assessment Decision Documents: - Comprehensive Security Reviews (CSR) - Periodic Security Reviews (PSR)	Area Manager[1] Regional Director[1] Chief Security Officer[1]
Security Issue Evaluation Decision Documents	Area Manager[1] Regional Director[1] Chief Security Officer[1] Director, SSLE[1]
Security Corrective Action Study Decision Documents	Area Manager Regional Director Chief Security Officer Director, SSLE Deputy Commissioner, PAB
NCI facilities – All Decision Documents (except PSRs) MMC facilities – Decision Documents that contain significant changes (except PSRs)	Area Manager Regional Director Chief Security Officer Director, SSLE Deputy Commissioner, PAB Commissioner AS/WS (Concurrence)

[1] May be further delegated at the discretion of the approving official, but may not be delegated lower than the facility manager.

13. **Consultation with Project Beneficiaries.**

A. Public Law 110-229, Section 513 requires the following:

(1) **Notice.** Reclamation shall provide project beneficiaries written notice describing the need for a new site security measure, describing the process for identifying and implementing the site security measure, and summarizing the administrative and legal requirements relating to the measure.

(2) **Consultation.** Reclamation shall provide project beneficiaries an opportunity to consult on the planning, design, and construction of the site security measure and on the development of timeframes for consultation.

(3) **Response.** Before incurring security-related reimbursable operation and maintenance costs, Reclamation shall consider cost containment measures recommended by a project beneficiary that has elected to consult with Reclamation on such activities. Reclamation will provide the project beneficiary a timely written response describing proposed actions, if any, to address the recommendations, and notice regarding the costs and status of such activities on a periodic basis.

B. Notice to, consultation with, and response to project beneficiaries are the responsibilities of the regional and/or area office responsible for the facility. The Regional Security Officer, with the assistance of the SSLE Security Office, will provide technical information and support regarding the need for the site security measure; planning, design, and construction; and estimated costs.

C. Upon identifying a new site security measure, the area manager will provide written notice and an opportunity to consult to project beneficiaries that have a direct responsibility to repay project operation and maintenance costs. Project beneficiary costs for consultation will be borne by the project beneficiary.

D. For operating entities that participate in the CSR or PSR that generates the site security measure, the CSR or PSR process meets the above requirements for notice, consultation, and response.

E. The final decision regarding implementation of site security measures rests solely with Reclamation.

F. Under emergency situations or elevated threat conditions, Reclamation may increase the levels of physical security protective measures, including guards and patrols, or adjust security procedures as appropriate without prior notice and consultation with project beneficiaries.

14. **Security System Design and Implementation.**

A. **Integrated Design.** Physical and/or technical security measures and systems shall be integrated to the greatest extent possible. Security measures, such as access control systems, automatic gates, video monitoring systems, intrusion detection systems, and command and control systems, shall wherever possible be integrated into a single, operator-friendly system. To further the efficient use of Reclamation resources, all systems shall, to the greatest extent possible, be designed to provide for monitoring by centralized security monitoring stations. Centralized monitoring will generally be limited to closely-related facilities (operationally and geographically) and complexes of such facilities. Broader-based centralized monitoring will be considered only after a thorough review of technical capabilities, including supporting telecommunications and information technology infrastructure.

B. **Design Preparation and Implementation.** The regional director, area manager, and Chief Security Officer will jointly determine responsibilities for security system design preparation and implementation, in fulfillment of recommendations approved in security-related decision documents. This includes responsibilities for design preparation, design approval, coordination, contracting, installation, and system integration and commissioning. Security system designs include, but are not limited to, facility hardening/protection, access control systems, perimeter barriers, video monitoring systems, intrusion detection systems, command and control systems, security control centers, and security-related procedures. The decision document must clearly delineate which person or office has responsibility for each action. The individual responsible for design approval will ensure that final designs are consistent with approved decision document recommendations.

C. **Design Standards.** All security system designs, and major modifications to designs or installed security systems, must be compliant with appropriate physical security standards, technical specifications, and best practices, including standards associated with the Federal Information Security Management Act (FISMA), FIPS-201, and North American Electric Reliability Corporation Critical Infrastructure Protection Standards (when applicable).

15. **Project Management.** Reclamation will utilize project management principles for security-related studies and fortification projects, as appropriate, based on the scope and complexity of the activity. SCASs and major fortification projects will often require a project management team (PMT). The study team leader, activity manager, or individual responsible for accomplishment of the fortification project will determine whether a PMT is needed, in collaboration with the Chief Security Officer and appropriate regional and area office managers. The size, scope, and membership of the team will be determined using the project management guidance contained in Reclamation's Security Risk Management Program guidelines.

16. **Additional Requirements.**

A. **Reimbursability.** Requirements for reimbursability of security costs can be found in the Reimbursability of Security Costs D&S at http://www.usbr.gov/recman/sle/sle05-01.pdf.

B. **Staffing.** Reclamation will provide technical security expertise and support for operations at all levels through the hiring or contracting of skilled professional security personnel. Each regional office will have an experienced Regional Security Officer who will be responsible for managing the overall regional security program. Each NCI facility will have an experienced facility security officer who is responsible for the day-to-day security guard functions and oversight of related security activities. The NCI facility security officer may also serve as the Area Office Security Coordinator. Each area office that does not have an NCI facility will have an Area Office Security Coordinator, which may be a collateral duty position.

C. **Site Security Plans.** A Site Security Plan (SSP) will be developed by the regional or area office for all facilities with a security criticality designation of Project Essential or higher. This requirement may be waived in an official decision document, particularly in cases where a transferred works operating entity has developed an SSP or an acceptable equivalent document. The plans will document security systems, procedures, and responsibilities for both normal operations and responses to threat conditions or other emergency security incidents. The plans will be integrated into, or used closely in conjunction with, Standing Operating Procedures, Emergency Action Plans, Continuity of Operation Plans, and other emergency occupancy and evacuation plans, as applicable (any highly-sensitive security information should remain in a separate document). A copy of the plan and any revisions shall be transmitted to all appropriate offices, including the SSLE Security Office (84-45000). SSPs or acceptable equivalent documents prepared by operating entities must be reviewed by the Regional Security Officer or Area Office Security Coordinator to ensure completeness and accuracy of the SSP.

D. **Security Guard Plans and Procedures.** Security guard plans and procedures will be developed and implemented by the area office, in consultation with the Regional Security Officer and Chief Security Officer, wherever full-time guards (armed or unarmed) are employed to protect a facility. At a minimum, the following plans are required: Security Guard Standing Operating Procedures, Post Orders, a Facility Defense Plan, and a Training Strategy to support these plans. A final copy of any guard plans and procedures, and any revisions, shall be transmitted upon approval to all appropriate offices, including the SSLE Security Office (84-45000). Security guard plans and procedures shall be implemented before guards are deployed.

E. **Annual Reviews and Training.** Regional or area office personnel must conduct annual reviews, inspections, and periodic tests of their Site Security Plans and security equipment, document the results of those reviews and tests, and conduct annual security awareness information or training for employees. For facilities where operation and maintenance has been transferred to an operating entity, these

requirements may be met by qualified operating entity personnel or performed jointly with Reclamation regional or area office personnel.

(1) SSPs must be reviewed at least annually to ensure procedures and contact information is accurate and complete.

(2) SSPs must be reviewed at Emergency Action Plan exercises and updated as appropriate to ensure accuracy and consistency with the Emergency Action Plans and Standing Operating Procedures.

(3) Security scenarios must be used as the primary Emergency Action Plan exercise scenario at least once every third exercise.

(4) Annual security inspections must be conducted of electronic security systems, such as security sensors, video surveillance, access control systems, and other alarm systems; and physical security systems, such as barriers, fencing, locks, and gates; to ensure functionality and operability. This action is not required for electronic equipment that has periodic or continuous self-checks, or physical systems that are operated on a routine basis. The requirement for annual checks must be documented in the facility Standing Operating Procedures. This process must be integrated with the facility's Annual Inspection process for other facility equipment.

(5) All Reclamation employees and contractors will periodically receive security awareness information or training that covers general and specific security topics. To support this requirement, the Reclamation Security Working Group will annually identify a theme and, with assistance and support from SSLE, help develop and provide current and relevant security awareness material for distribution of products, such as on-line security awareness training, talking points, brochures, and newsletters. This information and/or training will be provided to employees and contractors annually by the Regional Security Officers, in coordination with Area Office Security Coordinators. Where necessary to address local conditions, Regional Security Officers, in coordination with Area Office Security Coordinators, will develop and implement specific localized security awareness training activities to supplement the annual security awareness information or training. The local training activities must be pertinent to the roles and responsibilities of personnel at the facility, such as information security, tourism security, and observation and reporting of incidents and suspicious activities. The local training activities shall include content, delivery methods, and schedules that meet the unique operational needs of the region, area offices, and facilities.