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 (Pub. L. 107-56; 115 Stat. 272; 42 U.S.C. 5195c); Homeland Security Act of 2002 (Pub. L. 107-296; 116 Stat. 2135; 6 U.S.C. 101); Consolidated Natural Resources Act of 2008, Section 513, Bureau of Reclamation Site Security (Pub. L. 110-229; 122 Stat. 755; 43 U.S.C. 373e); Executive Orders 10450, 10577, 12958 as amended, and 12968; Homeland Security Presidential Directives; Federal Information Processing Standards 200 and 201; and Departmental Manual (DM) Parts 442, 444 and 446.

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

Contact: SSLE, 84-450000

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 risks at Reclamation facilities. This D&S prescribes minimum security requirements and processes for the physical security of Reclamation facilities.

2. **Applicability.** This D&S applies to Reclamation employees responsible for the management, assessment, security, operation, or maintenance of facilities and buildings owned by Reclamation.

3. **Definitions.** In addition to the following definitions, a list of common acronyms used in this D&S is provided in Paragraph 12.

   A. **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." This definition forms the basis for security criticality designations of Reclamation facilities (see Paragraph 5).

   B. **Security System.** Electronic or physical equipment, components, or devices intended for any of the following purposes:

      (1) control of access to a Reclamation facility,

(2) delay, detection, deterrence, or assessment of unauthorized access to, or misuse of, Reclamation facilities,

(3) mitigation of, or response to, risk from attack on Reclamation facilities, employees, or visitors, and

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

4. **Responsibilities.** Overall security responsibilities are listed in the Reclamation Manual Policy, *Security Program* (SLE P01). Responsibilities related to facility security are as follows:

A. **Director, SSLE.** The Director, SSLE is responsible for:

(1) developing, implementing, and managing Reclamation's Security Program, including the facility security component; and

(2) ensuring that the Commissioner, Deputy Commissioners, and the Assistant Secretary – Water and Science (AS/WS) are notified of any significant facility security issues, including road closures, major changes in security posture, or major changes in risk factors.

B. **Regional Directors.** Regional directors are responsible for:

(1) managing and overseeing the Security Program throughout their respective regions;

(2) ensuring security equipment is adequately maintained in an operational state and is fully utilized; and

(3) keeping the Director, SSLE informed of significant facility security issues, including road closures, major changes in security posture, or major changes in risk factors.

C. **Area and Facility Managers.** Area and facility managers are responsible for:

(1) the daily operation and maintenance of security equipment and management of guard forces and/or contracts;

(2) ensuring security equipment is adequately maintained in an operational state and is fully utilized and that facility staff follow all security procedures; and

(3) ensuring necessary actions to reduce risk are communicated to project beneficiaries in accordance with Pub. L. 110-229, Section 513, and that these entities have an opportunity to participate in the development of risk reduction alternatives.

D. **Chief Security Officer (CSO).** The CSO is the principal staff person responsible for:

(1) formulating, coordinating, managing, operating, and overseeing Reclamation's Security Program;

(2) serving as the Security Program Manager as described in 444 DM 1;

(3) oversight of all facility Security Program activities except weapons, explosives, and ammunition, for which Reclamation's Special Agent-in-Charge has oversight responsibility; and

(4) implementing a security assessment program to support facility security risk mitigation activities, including periodic reviews, studies, and associated decisionmaking.

E. **Regional Security Officers (RSOs).** RSOs are responsible for:

(1) coordinating, managing, and overseeing facility security functions within their regions, including implementing risk reduction strategies and facility security protection measures, oversight of guard functions, and regional budget planning and execution;

(2) providing support to the area manager and regional director for ensuring security equipment is adequately maintained in an operational state and is fully utilized for its intended purposes;

(3) implementing security awareness programs throughout their respective regions; and

(4) ensuring significant changes in risk factors are reported to the Chief Security Officer in a timely manner, such as changes in the population downstream of a dam, emerging threat or incident information, changes in structural vulnerability, or changes in the status of security equipment or protective measures.

F. **Regional Special Agents (RSAs).** RSAs are responsible for:

(1) supporting Reclamation's facility security activities by coordinating and interfacing with other law enforcement and intelligence agencies within their respective regions;

(2) conducting and updating threat assessments;

(3) participating in security reviews;

(4) assisting in the oversight of guard functions;

(5) conducting investigations; and

(6) providing information on threats and incidents that could affect the security of Reclamation facilities.

G. **Area Office Security Coordinators (AOSC).** AOSCs are responsible for:

(1) coordinating and overseeing security functions within their area office;

(2) providing support to the area manager, RSO, and regional director by ensuring security equipment is adequately maintained in an operational state and is fully utilized for its intended purposes;

(3) implementating security awareness programs throughout their respective area offices, within the framework established by the RSO, and for ensuring Site Security Plans are maintained and coordinated with Emergency Action Plans, Emergency Management Program, and other similar programs;

(4) ensuring tour guides and visitor center personnel receive periodic training in security awareness and tourism security and safety;

(5) promptly reporting security issues and ensuring significant changes in risk factors that might affect facility security are reported to the RSO in a timely manner; and

(6) Promptly reporting completion of recommendations and status updates to SSLE.

5. **Security Criticality Designations.** The following security designations are used by Reclamation to characterize the relative criticality of all Reclamation facilities. Criticality designations are determined based on a range of factors such as population at risk, structure type and size, and the impacts that the incapacity or destruction of each facility would have. A change in designation may be initiated by either the regional office or SSLE, but must be made through a formal decision document which contains a recommendation and justification for the change. SSLE will maintain the official list of criticality designations. A general description of each designation is provided below based on the definition of critical infrastructure contained in the Critical Infrastructure Protection Act of 2001.

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.** 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. **Security Measures.** Reclamation will implement, operate, and maintain physical security measures as determined by Reclamation decision documents and applicable Federal policies and standards, including those listed below:

A. **DM Minimum Security Standards.** DM Part 444 prescribes minimum security standards that must be applied at all Department of the Interior facilities, including requirements for physical security measures, security assessments, and security plans.

(1) **444 DM 1 – Physical Security Program Requirements.** 444 DM 1 applies to buildings occupied by Reclamation employees and contractors. 444 DM 1 requires that Department bureaus and offices utilize the Interagency Security Committee (ISC) documents titled *"Facility Security Level Determinations for Federal Facilities"* and *"Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard***"** as minimum requirements for physical security at Department facilities.

(2) **444 DM 2 – NCI and Key Resource Security.** 444 DM 2 applies to NCI facilities and other facilities of national significance, including Reclamation's five NCI facilities. 444 DM 2 contains minimum physical security requirements, and requirements for security risk assessments, surveys, and security plans.

(3) **444 DM 5 – Other Structures.** 444 DM 5 contains minimum security requirements for Departmental structures not meeting the criteria defined in 444 DM 1 or 444 DM 2. The Department Office of Law Enforcement and Security has determined that Reclamation's project facilities (dams, powerplants, water conveyance structures, etc.) fall under 444 DM 5 (except for NCI facilities).

B. **Decision Documents.** Physical security measures at Reclamation facilities are collaboratively determined through a formal risk assessment and decisionmaking process. Recommendations from these assessments are approved in formal decision documents. These processes are described in Paragraphs 7 and 8 of this D&S. Paragraph 8.C. provides the specific approval levels for the various decision document types.

C. **Threat Condition Protective Measures.** Reclamation's Threat Condition Protective Measures are additional security measures that are placed in service based on the Department of Homeland Security National Terrorism Advisory System. These measures vary based on the threat alert level issued by the Department of Homeland Security. A copy of Reclamation's Threat Condition Protective Measures can be obtained from the CSO or RSO.

D. **Federal Information Processing Standards (FIPS) 200.** 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 components that communicate via the TCP/IP protocol, are physically connected to the local EACSS network, are assigned unique IP addresses, and have login capability within the EACSS deployment.

E. **FIPS-201.** All electronic access control 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, specifications, and guidelines.

F. **North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards.** The NERC-CIP Standards contain minimum requirements for the protection of Critical Cyber Assets in support of the reliability of the bulk electric system.

G. **ASTM Standard F2766-11 – Standard Test Method for Boat Barriers.** This ASTM standard prescribes the standard test method for boat barriers intended for the mitigation of risk to critical assets from attack by water-borne surface vessels commonly found on reservoirs and rivers. The following or a similar clause shall be included in all contracts for the procurement of a boat barrier system proposed for installation on Reclamation facilities for the above purpose: "The contractor shall, for any boat barrier proposed for supply and/or installation under this contract, provide the contracting officer with proof of certification in accordance with ASTM Standard F2766-11 – Standard Test Method for Boat Barriers. This proof of certification shall be provided to the contracting officer as part of any contractor proposal for the supply and/or installation of any boat barrier proposed under this contract." This requirement does not apply to buoy lines and barriers installed for other purposes such as boater safety or demarcation.

7. **Security Assessments.** Reclamation will maintain a security assessment program that ensures security reviews are completed periodically for all NCI, MMC, MC, and PE facilities. In addition, buildings occupied by Reclamation employees will have security assessments as required by 444 DM 1.

   A. **Assessment Type and Frequency.** The following table lists the assessment types and required assessment frequency for each facility level. The assessment types and associated requirements are described in Paragraphs B through G. (In the table below, CSR stands for Comprehensive Security Review and PSR stands for Periodic Security Review.)

	Facility Level	**Assessment Type**	**Required Frequency**
Required Periodic Reviews	NCI	CSR and PSR	Alternating every 3 years
	MMC	CSR and PSR	Alternating every 4 years
	MC	PSR	Every 4 years
	PE	PSR	Every 8 years
	NCI, MMC, MC, PE	Security Equipment Inspection	Annually
	Level 1 and 2 Buildings[1]	ISC Physical Security Criteria Review	Every 5 years as required by 444 DM 1
	Level 3 and 4 Buildings[1]	ISC Physical Security Criteria Review	Every 3 years as required by 444 DM 1
Issue-Specific Reviews	All	Security Issue Evaluation (SIE)	As needed
		Security Corrective Action Study (SCAS)	As needed
Supporting Assessments	All	Risk Analysis (numerical rating of relative asset risk)	As needed to support other assessments
		Threat Assessment	As needed to support other assessments
		Readiness Effectiveness Assessment	Optional
		Exercise After-Action Reports	In conjunction with major exercises

[1] Building security levels are determined using the ISC Standard: *Facility Security Level Determinations for Federal Facilities*.

B. **Comprehensive Security Review (CSR).** A CSR is utilized to evaluate the potential risks to the public, Reclamation staff, and Reclamation facilities resulting from a human attack or other criminal activity. The CSR reviews security measures and procedures in place, potential threats, structural and procedural vulnerabilities, and consequences of loss, including loss of life and economic losses. The resulting assessment and estimation of risks is used to identify appropriate risk-reducing actions and provides a relative priority for funding mitigation activities.

(1) A CSR will be conducted every 6 years for each NCI facility and every 8 years for each MMC facility. The SSLE Security Office will facilitate the scheduling of CSRs to ensure periodic review requirements are met.

(2) A CSR is not required on a regularly scheduled basis for MC and PE facilities. However, a CSR will be conducted if a PSR or other risk assessment determines that a CSR is needed or at the request of facility, area office, regional, or SSLE management.

(3) Accomplishment of CSRs is the responsibility of the CSO. The CSO, or his/her designee, will assign a CSR Team Lead for each review. Each CSR team will include the Deputy CSO or an SSLE physical security specialist plus additional members from the Technical Service Center (TSC), regional office, area office, and facility (including transferred works personnel) as needed.

(4) A CSR will consist of a review and update of the previous CSR conducted for the facility. A site visit is required for each CSR.

(5) A risk analysis will be conducted, or the previous risk analysis updated, as part of the CSR.

(6) CSR findings, including any recommended mitigation actions, will be documented in a CSR report and decision document. Each recommendation will include the projected cost, funding source, viable target completion date, and responsible party. If the CSR determines that significant issues exist that cannot be resolved in the CSR, the report must include a recommendation to conduct an SIE or SCAS to address those issues.

(7) The CSR report will be reviewed by a security advisory team which will include the CSR team leader, an SSLE Security Office representative, a manager or other representative from the area office and/or facility, and other staff as necessary. The recommended decisions made by the security advisory team will be documented within the CSR report which will serve as the decision document that is transmitted to the approving officials.

C. **Periodic Security Review (PSR).** A PSR is utilized to evaluate the security measures and practices in place at a facility with respect to the operational effectiveness, utilization, and maintenance of security system equipment and consistency with security procedures in the facility Site Security Plan. The PSR is not intended to address significant issues or make recommendations for major mitigation actions; however, recommendations for minor fortification upgrades or additions can be included for consideration. If the PSR determines that significant issues exist or major mitigation actions are necessary, the PSR must include a recommendation to conduct a more comprehensive risk assessment, such as a CSR or SIE. The final PSR report will serve as the decision document.

(1) A PSR will occur every 4 years for each MC facility and every 8 years for each PE facility. A PSR will alternate with a CSR every 3 years at an NCI facility and every 4 years at an MMC facility.

(2) A PSR will consist of a review and update of the previous PSR conducted for the facility. A site visit is required for each PSR.

(3) Accomplishment of PSRs is the responsibility of the RSO and will involve personnel from the regional office, area office, and/or facility, including transferred works personnel as appropriate.

(4) PSR findings, including any recommended mitigation actions, will be documented in a PSR report using the standard PSR report template. Each recommendation will include the projected cost, target completion date, funding source, and responsible party. The final PSR report will serve as the decision document.

(5) The RSO will post the draft report on the Security SharePoint site and notify the Deputy CSO that it is ready for review.

(6) A security advisory team review is not required for a PSR; however, if the PSR contains fortification recommendations, it must be reviewed by the CSO or Deputy CSO before signature of the area manager and regional director.

(7) For NCI, MMC, and MC facilities, the PSR will include a specific determination as to whether the PSR meets the current risk assessment needs for the facility, or whether a more detailed CSR or SIE is needed. If there is a determination that a more detailed risk assessment is needed, it shall be documented as a recommendation in the PSR, including the type of assessment and schedule for completion.

D. **ISC Physical Security Criteria Review.** Buildings and structures occupied on a regular basis for the majority of the normal work day by Reclamation employees and contractors are subject to a minimum security standards review as required by 444 DM 1. This review must be conducted utilizing the *"Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard."* This review is not required for buildings and structures where the minimum standards are evaluated as part of a CSR or PSR. Accomplishment of an ISC review is the responsibility of the RSO in consultation with area office and facility personnel as appropriate. Completion of the ISC review must be documented, but a formal report and decision document is not required.

E. **Security Issue Evaluation (SIE).** An SIE is utilized to evaluate a specific security issue and potential alternatives to mitigate the issue. Issues requiring an SIE are usually identified through CSR or PSR recommendations, but are also triggered by risk factor surveys, security-related incidents, exercises, general research, or proposed changes to previous decisions or security posture, such as changes in security guard strategies or significant changes to visitor tours. SIEs and resulting reports can vary greatly in size and resource needs depending on the scope and complexity of the issue, and as a result, an SIE may be large in scope (e.g., a study of embankment mitigation alternatives) or small in scope (e.g., an evaluation of fencing alternatives to complete a CSR recommendation).

(1) For large or complex evaluations, a project team will be established to plan and accomplish the SIE. The project team leader will generally be from the area office or region where the project is located. The project team will include the RSO, TSC staff, and SSLE staff as needed to accomplish the study.

(2) An SIE decision document will be prepared by the team conducting the evaluation. At a minimum, the decision document must include a baseline risk analysis and a discussion of the alternatives, including pros and cons, estimated risk reduction, and cost. It must also contain 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.

(3) The team must determine whether the SIE report and decision document will go through a peer review, security advisory team review, and/or a value engineering study, based on the scope, cost, and complexity of the issues and recommendations.

F. **Security Corrective Action Study (SCAS).** An SCAS is utilized when a comprehensive analysis of a security-related issues and mitigation alternatives is needed, including costs and projected risk reduction. An SCAS will usually be initiated through an SIE decision document, but can also be formally recommended through any decision process providing sufficient justification.

(1) A project team will be established to plan, manage, and accomplish the SCAS. The project team leader will generally be from the area office or region where the project is located. The project team will include the RSO, TSC staff, and SSLE staff as needed to accomplish the study.

(2) An SCAS decision document will be prepared by the team conducting the study. At a minimum, the decision document must include a baseline risk analysis and a detailed discussion of the alternatives, including pros and cons, estimated risk reduction achieved, and a feasibility-level design and cost estimate. It must also contain a recommended decision and supporting justification to either rely on current security measures in place (take no action) or to implement specific mitigation actions.

(3) During development of an SCAS that identifies mitigation action alternatives that involve physical modification to existing facilities or other construction or ground disturbing actions, consultation shall occur with the appropriate Reclamation environmental and cultural resources management professionals.

(4) Proposed mitigation measures are subject to applicable technical peer reviews, value engineering studies, and design, estimating, and construction studies as required by RM Policy and D&S.

G. **Other Supporting Reviews and Assessments.** The following assessments provide supporting information and data for CSRs, PSRs, SIEs, and SCASs.

(1) **Annual Security Equipment Inspection.** All security equipment shall be inspected annually to ensure the functionality, operability, maintenance, and utilization of the equipment. Security equipment includes electronic security systems and components, such as security sensors, servers, cameras and monitors, access control systems, and alarm systems; and physical security systems, such as barriers, fencing, locks, and gates. This inspection will be conducted as part of the annual site inspection of significant- and high-hazard dams, the annual facility review of power and associated facilities, or a separate site security inspection as determined by the regional and area offices. The results of this inspection shall be documented and provided to the RSO.

(2) **Risk Analysis.** A security risk analysis evaluates the perceived threats, vulnerabilities, consequences, and security measures at a facility. It provides a relative risk rating for each critical facility asset. This rating is used to prioritize Reclamation-wide mitigation activities and to provide a relative quantification of risk to aid decisionmakers in determining if a mitigation action is warranted for a specific asset. The risk analysis is reviewed and updated by SSLE staff, in collaboration with appropriate regional and area office staff, prior to CSRs, SIEs, and SCASs if needed, and as changes in site factors occur that might affect the risk rating of a facility. The risk analysis is also updated after mitigation activities have been completed at a facility.

(3) **Threat Assessments.** A threat assessment evaluates potential security-related threats to a facility, including potential types of attack, aggressor capability, and intent. These assessments are based on a combination of local, regional, and

international threat and intelligence information. A threat assessment will be conducted as needed in support of risk assessments or in response to critical intelligence indicators or management concerns. Threat assessments will be conducted by the RSAs with the support of the SSLE Information Sharing and Law Enforcement staff. The findings of a threat assessment must be documented, including any numerical threat rating required by a facility-specific risk assessment.

(4) **Readiness Effectiveness Assessment.** A readiness effectiveness assessment is a structured, formal assessment of the effectiveness of an approved and fielded security system's cumulative capability to mitigate a given threat. These assessments can include functional tests of security systems, guard force interaction, or staff interaction to detect suspicious activities and to deter, detect, delay, or deny potential threats. These tests will be conducted under the auspices, control, and safety oversight of the SSLE Director, Regional Director, and Special-Agent-in-Charge. The assessment must be vetted and coordinated with the RSO and RSA in advance of the assessment. A decision document is required if the assessment report contains physical security recommendations or a recommendation to conduct additional reviews or studies.

(5) **Exercise After-Action Report.** An exercise after-action report contains a summary of the findings and recommendations from an emergency planning exercise. The exercise can range anywhere from a routine Emergency Action Plan exercise to a full-scale security and law enforcement exercise. A decision document is required if the assessment report contains physical security recommendations or a recommendation to conduct additional reviews or studies.

H. **Recommendation Tracking.** All risk assessment recommendations will be recorded and tracked in the Security Risk Assessment Database maintained by SSLE. SSLE will send a recommendation tracking report to each region on a quarterly basis; the AOSC will update the status of recommendations and provide the updated data to SSLE.

I. **Risk Assessments by External Entities.** Many different entities, including the Department of Homeland Security, State Offices of Homeland Security, National Guard, 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 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 RSO for coordination and approval. The RSO is responsible for informing the CSO of the request and proposed response.

8. **Decisionmaking Process.**

A. **Decision Document.** Written documentation of each recommended mitigation action, final decision, and supporting justification is required. If there is a decision that warrants action by Reclamation, then at a minimum the documentation will describe the decision, including the actions, timeframes, estimated cost, funding sources, and responsible office. If a decision is made to take no action on an issue or recommendation, then that decision will be documented with supporting justification. Subsequent changes to a decision document after obtaining any signatory's concurrence will be re-vetted by all approval authorities prior to final signature.

B. **Significant Issues at MMC Facilities.** If a decision document for an MMC facility addresses significant issues, it elevates the required concurrence level (see table below). Significant issues include significant public impact such as road restrictions, closures, or openings; major fortification activities; significant cost outlays; major operational changes (e.g., significant security guard force modifications); and major changes in threat, vulnerability, or consequences. However, if the decision document only recommends additional evaluation of the significant issues, concurrence is not required above the SSLE Director.

C. **Concurrence Levels.** Security risk assessment decision documents require signatory concurrence at the following levels.

		Area Manager[1]	Regional Director[1]	Chief Security Officer[1]	SSLE Director[1]	Deputy Comm. PAB[2]	Comm. and AS/WS[3]
PSR	PE, MC, MMC, NCI	✓	✓	✓			
CSR	MC, MMC	✓	✓	✓			
	MMC w/significant issues	✓	✓	✓	✓	✓	✓
	NCI	✓	✓	✓	✓	✓	✓
SIE	PE, MC, MMC	✓	✓	✓	✓		
	MMC w/significant issues	✓	✓	✓	✓	✓	✓
	NCI	✓	✓	✓	✓	✓	✓
SCAS	PE, MC	✓	✓	✓	✓	✓	
	MMC, NCI	✓	✓	✓	✓	✓	✓

[1] Document can be signed by a deputy manager or deputy director

[2] Deputy Commissioner, Policy, Administration, and Budget

[3] Assistant Secretary for Water and Science

9. **Consultation with Project Beneficiaries.**

A. The consultation requirements of Pub. L. 110-229, Section 513 will be accomplished by the regional and/or area office responsible for the facility. The RSO, with the assistance of the SSLE Security Office, will provide technical information and support regarding the need for the site security measure and estimated costs.

B. Upon identifying a new site security measure, the area manager will provide 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.

C. For project beneficiaries that participate in a security assessment that generates the site security measure, the security assessment process meets the requirements for notice, consultation, and response.

D. Prior notice and consultation is not required in order to increase the levels of physical security protective measures, such as guards and patrols, under emergency situations or elevated threat conditions.

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

A. **Design of Security Systems.**

(1) **Consistency with Decision Documents.** All security system designs and equipment must be commensurate with the approved recommendations in risk assessment decision documents. New security systems or equipment shall not be installed and existing systems significantly upgraded or modified without an approved decision document as described in this D&S.

(2) **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 be, wherever possible, integrated into a single, operator-friendly system. The design process shall also 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 24/7 monitoring, assessment, and dispatch functions, either at a government or a commercial central monitoring station.

(3) **FIPS and NERC-CIP Standards.** All security systems shall be designed, procured, installed, and operated in compliance with applicable FIPS and NERC-CIP Standards. All Reclamation access control systems shall use the Homeland Security Presidential Directive 12 / FIPS-201 Federal smart card credential as the only official means of identity authentication and physical access control. Design, procurement, and installation of new access control systems shall be fully FIPS-

201 compliant. Existing access control systems shall be brought into FIPS-201 compliance in accordance with Departmental policy and guidance.

(4) **Design Approval.** Security system designs must be approved by an SSLE physical security engineer or physical security specialist before procurement. This will help ensure components are compatible; have a positive track record for reliability, maintenance, and ease of operation; comply with applicable industry, Federal, Department, and Reclamation physical security standards and information technology (IT) compliance requirements; and adhere to cost-effective procurement and operation and maintenance (O&M) strategies.

B. **System Components**. SSLE will maintain an inventory or mechanism for quickly procuring common security system components. SSLE physical security specialists shall be consulted before replacing security system components, unless identical components are available or have been previously approved. This includes components of access control systems, vehicle and boat barriers, video monitoring systems, intrusion detection systems, and other security-related products. The consultation will determine if SSLE can provide funding from the replacements budget and will ensure replacement equipment is the most effective and cost efficient product available, and complies with applicable industry, Federal, Department, and Reclamation physical security standards and IT compliance requirements.

C. **Project Management.** Major fortification projects, including structural modifications, will usually require a project management team to oversee the design, procurement, construction, installation, and acceptance of the project. The project team leader will generally be from the area or regional office where the project is located and involve facility staff, procurement staff, RSO, SSLE physical security specialists, and others, as appropriate, based on the scope and complexity of the activity.

D. **O&M of Security Systems.** All security systems and equipment will be fully utilized, monitored, and maintained.

(1) All equipment will be maintained in good working order to maximize security effectiveness and longevity (e.g., cleaning and calibration of cameras).

(2) Equipment malfunction and/or outages will be immediately reported to facility maintenance staff or entered into maintenance tracking systems following facility procedures. Significant malfunctions and outages of system equipment or functionality defined as critical to system readiness and effectiveness must be immediately reported to the facility manager and the AOSC.

(3) Security system alarm and error logs shall be reviewed at least monthly to identify system issues and anomalies. IT security and system event logs must be reviewed in accordance with documented policies and procedures. All system issues and anomalies will be documented, investigated, and corrected in a timely manner.

(4) A summary of significant outages and failures and actions taken must be included in the area office annual report (see Paragraph 11.A.).

(5) The area office shall maintain a compilation of all baseline inventories for the area office. The inventories shall be used to develop out-year O&M budget projections for the security systems and to coordinate with the RSO on outyear equipment replacement needs. Budgeting and reimbursability of O&M costs are covered in the RM D&S *Reimbursability of Security Costs* (SLE 05-01).

(6) Changes to the baseline system inventory or changes to the configuration of the baseline system shall comply with the change management process as required by applicable industry, Federal, Department, and Reclamation IT compliance requirements.

(7) The area office will develop and implement a site-specific security system O&M plan as described below in Paragraph 10.E. The plan will be reviewed and approved by the RSO and a copy of the approved plan shall be submitted to the SSLE Security Office. For new security system installations, the security system plan shall be completed within 90 days of project completion. For existing systems, the security system plan shall be completed as soon as possible to support ongoing O&M activities.

E. **Security System O&M Plan.** SSLE will provide assistance with development of the baseline system inventory, recommended maintenance procedures and schedules, and budgetary maintenance and replacement costs. SSLE will also provide plan templates and sample plans from similar facilities. The site-specific security O&M plan shall include the following information:

(1) Procedures and practices for:

(a) granting, monitoring, and removing security system and facility access privileges for employees, contactors, and visitors;

(b) scheduling and performing preventative maintenance tasks, including those related to IT security;

(c) monitoring, reporting, and responding to equipment malfunctions and/or outages;

(d) monitoring, reporting, and responding to security system intrusion detection alarms;

(e) reviewing system alarm and error/failure logs affecting system readiness/effectiveness;

(f) reporting, tracking, and correction of issues and anomalies discovered during planned or emergency maintenance of the system;

(g) informing system administrators, the area office security coordinator, area manager, RSO, and the CSO of issues affecting system readiness or effectiveness; and

(h) training of security system users, operators, and administrators

(2) A baseline inventory of all systems, components, and devices. Items with a value greater than $500 or critical (single point of failure) to the readiness and effectiveness of the security system shall be included as an individual line items in the inventory. Other non-critical and low cost items may be rolled up into groups of like items and summarized as a single line item. The inventory shall include the following information for each line item:

(a) equipment type, manufacturer, model, and serial number;

(b) procurement cost;

(c) installation cost;

(d) initial or replacement installation date;

(e) expected useful service life;

(f) Designation as a critical or non-critical component;

(g) preventative maintenance tasks, frequency of task performance, and time to perform; and

(h) testing, calibration, and configuration tasks, frequency of task performance and time to perform

11. Additional Requirements.

A. **Area Office Annual Security Report.** Completion of an Area Office Annual Security Report is described in D&S FAC 01-06. The Area Office Annual Security Report will include a list of all area office facilities and buildings that have a periodic security review requirement (see Paragraph 7A) and the status of those reviews. At a minimum, the information shall include:

(1) General Information.

(a) Name of each facility and building.

(b) Facility criticality level or ISC building security level.

(c) Status of the Site Security Plan (or Facility Security Plan) and the Security System O&M Plan (i.e., do they exist and when were they last reviewed/updated?).

(2) Status of Security Reviews.

(a) Completion date of the last annual equipment inspection.

(b) Completion date of the last periodic review and the type of review completed (e.g., PSR with site visit).

(c) Status of any additional reviews or assessments conducted during the fiscal year (e.g., SIE, SCAS).

(3) Summary of Accomplishments.

(a) Fortification and mitigation activities.

(b) Significant changes (guard strategies, tours, procedures, etc.).

(c) Training, security-related exercises.

(d) Site Security Plans, Security System O&M Plans, etc.

(4) Summary of Issues.

(a) Security-related incidents and suspicious activities that occurred during the fiscal year.

(b) Significant issues and deficiencies that affect security system effectiveness.

(c) Significant issues and deficiencies identified during routine operation and maintenance and the status of issue correction.

(5) Any other pertinent security or law enforcement information that should be included in the Reclamation-wide Annual Security Report or reported for internal control purposes.

B. **Site Security Plans (SSP).** A SSP must be developed by the regional or area office for all NCI, MMC, MC, and PE facilities. The SSP must document security systems, procedures, and responsibilities for both normal operations and responses to threat conditions or other emergency security incidents. The SSP will be integrated into, or used closely in conjunction with, standing operating procedures and/or emergency action plans (any highly-sensitive security information must remain in a separate document). If the SSP is fully integrated into standing operating procedures or emergency action plans, a separate SSP is not required.

(1) SSPs must be reviewed at least annually to ensure security systems and procedures are adequately defined and up to date, contact information is accurate and complete, and information is consistent with emergency action plans and standing operating procedures (if the SSP is not integrated into those documents). This review will be annotated and available for compliance reviews as needed.

(2) SSPs or acceptable equivalent documents prepared by operating entities must be reviewed by the RSO or AOSC to ensure completeness and accuracy of the SSP.

(3) A copy of the SSP and any revisions shall be transmitted to the SSLE Security Office.

C. **Emergency Action Plan Exercises.** One of every three emergency action plan exercise scenarios must include a security scenario as a primary focal point.

D. **Facility Security Plans.** For buildings and facilities not associated with project facilities (e.g., office buildings) the ISC document titled *Physical Security Criteria for Federal Facilities — An Interagency Security Committee Standard* contains the following criteria: "Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System." Depending on building ownership and tenancy, the facility security plan is developed by the owner (e.g., General Services Administration), a facility security committee, or Reclamation. If the facility security plan is fully integrated into an occupant emergency plan or continuity of operation plan, a separate facility security plan is not required.

E. **Security Guard Plans and Procedures.** Security guard plans and procedures will be developed and implemented by the area office wherever full-time guards (armed or unarmed) are employed or contracted by Reclamation. At a minimum, the plans and procedures will include security guard standing operating procedures, post orders, a training strategy to support these plans, and use-of-force requirements contained in 444 DM 4. The plans and procedures will be provided to the CSO, RSO, and Special Agent-in-Charge for initial review, and anytime thereafter upon request. Security guard plans and procedures shall be implemented before guards are deployed, except in emergency situations.

F. **Staffing.** The CSO will serve as the security program manager as described in 444 DM 1. In addition, each regional office will have an experienced RSO who will be responsible for managing the overall regional security program. Each NCI facility will have an experienced full-time facility security officer who is responsible for the day-to-day security guard functions and oversight of security activities. The NCI facility security officer position must be dedicated to the security function and must not be encumbered with other significant duties, such as safety and emergency management.

Each area office that does not have an NCI facility security officer will have an AOSC, which may be a collateral duty position.

G. **Security Awareness Training.** RSOs, in coordination with RSAs and AOSCs, will develop and conduct specific security awareness training to address local facility needs, such as tourism security, information security, operations security, observation and reporting of incidents and suspicious activities, active shooter training, and facility orientations and risk briefings for first responders.

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

(1) Reclamation's Visitor Center Guidelines, issued by 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.

(2) All changes to public tours that have a significant security-related impact require a security issue evaluation and decision document as described in Paragraph 7.E.

(3) Tour guides and visitor center personnel must receive initial and periodic training in security awareness and tourism security. This training is the responsibility of the NCI Security Officer or AOSC.

(4) All non-public tours (such as school groups, technical groups, and international groups) must be scheduled with the facility in advance of the tour in order to obtain a list of tour participants and determine the tour route and information that will be provided and/or discussed. The RSO or AOSC must be notified of the tour, as far in advance as possible.

(5) Additional guidance regarding non-public tours of Reclamation facilities is available from the RSO or the SSLE intranet site.

(6) For additional requirements associated with visits by foreign nationals, please see RM D&S NIA 01-01, *Reclamations International Affairs Program*, which relates to Native American and International Affairs Office reporting requirements.

12. Acronyms

AOSC	Area Office Security Coordinator
AS/WS	Assistant Secretary for Water and Science
CIP	Critical Infrastructure Protection
CSR	Comprehensive Security Review
D&S	Directives and Standards

DM	Departmental Manual
EACSS	Electronic Access Control and Surveillance System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
ISC	Interagency Security Committee
IT	Information Technology
MC	Mission Critical
MMC	Major Mission Critical
NCI	National Critical Infrastructure
NERC	North American Electric Reliability Corporation
O&M	Operation and Maintenance
PE	Project Essential
PSR	Periodic Security Review
RSA	Regional Special Agent
RSO	Regional Security Officer
SCAS	Security Corrective Action Study
SIE	Security Issue Evaluation
SSLE	Security, Safety, and Law Enforcement
SSP	Site Security Plan