DRAFT RECLAMATION MANUAL RELEASE

Comments on this draft release must be submitted to rschuster@do.usbr.gov by September 15, 2008.

Background and Purpose of the Draft Facility Security Directive and Standard

The goal of this Directive and Standard is to establish facility security requirements for the Bureau of Reclamation. The benefits of this Directive and Standard are consistent application of security standards and procedures at Reclamation facilities.

The Reclamation Manual is used to clarify program responsibility and authority and to document Reclamation-wide methods of doing business. All requirements in the Reclamation Manual are mandatory.

See the following pages for the draft Directive and Standard.

DRAFT RECLAMATION MANUAL RELEASE
Comments on this draft release must be submitted to rschuster@do.usbr.gov by September 15, 2008.

SLE 03-02

Reclamation Manual

Directives and Standards

Subject: Facility Security

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

Authority: Reclamation Act of 1902, as amended and supplemented; Critical Infrastructure Protection Act of 2001; Homeland Security Act of 2002; Homeland Security Presidential Directive 7; and Departmental Manual (DM) Part 444.

Approving Official: Director, Security, Safety, and Law Enforcement

Contact: Security, Safety, and Law Enforcement Office (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 risks and protecting Reclamation's employees, 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 all 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.

3. **Responsibilities.** Overall responsibilities for the Security Program are established in Reclamation Manual Policy, *Security Program* (SLE P01). Implementation of this D&S is the responsibility of the appropriate Director, Regional Director, or Area Manager.

4. **Security Measures.** Facility personnel will implement and maintain physical security measures as directed by Departmental Manual (DM) Minimum Security Standards, Reclamation security Decision Documents, Reclamation's Threat Condition Protective Measures, appropriate security-related procedures, and other applicable Federal standards.

   A. **Departmental Manual 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 Interior 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 SLE P01. 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 – National Critical Infrastructure Facilities
Security Level 4 – Major Mission Critical Facilities
Security Level 3 – Mission Critical Facilities
Security Level 2 – Project Essential Facilities
Security Level 1 – Low-risk facilities

(2) **Buildings and Offices.** Reclamation must apply the procedures of 444 DM 1 for determining the most appropriate level of security for a building or office. The security level of a building, office, or similar facility is based on factors such as 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 of a Reclamation facility determine what security measures are required in addition to the minimum security standards prescribed in the DM. Final approved recommendations are documented in a formal Decision Document. Significant security decisions that are made outside the risk assessment process must also be documented in a supplemental Decision Document or Decision Memorandum. The Security Risk Assessment and Decisionmaking processes are described in SLE P01.

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. 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 appropriate Regional Security Officer.

D. **FIPS-201.** All electronic access control systems purchased or deployed by Reclamation after February 19, 2004, must be compliant with the Federal Information

Processing Standard Publication 201, *Personal Identity Verification of Federal Employees and Contractors*, and related implementing standards and specifications.

5. **Security System Design and Implementation.**

   A. **Integrated Design.** Physical 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.

   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 Decision Documents. This includes responsibilities for design preparation, coordination, contracting, installation, and system integration and commissioning. Security system designs include, but are not limited to, hardening/protection of controlled access areas, access control systems, perimeter barriers, video monitoring systems, intrusion detection systems, command and control systems, and security control centers. The Decision Document must clearly delineate which person or office has responsibility for each action.

   C. **Design Approval.** All security system designs, and major modifications to designs or installed security systems, must be reviewed and approved by the Chief Security Officer to ensure compliance with appropriate physical security standards, technical specifications, and best practices. This review will be conducted by the SSLE Security Office in a timely manner. In some cases, the Chief Security Officer may determine that this review and approval is not required, based on the size and complexity of the system, use of standard specifications, and other factors.

6. **Project Management.** The Regional Director, Area Manager, and Chief Security Officer will collaboratively determine if specific security fortification projects require formal project management. The Regional Director, Area Manager, and Chief Security Officer will determine the scope and degree of project management to be applied (e.g., data gathering, design preparation, contracting, construction management, and resource accountability) and the Project Manager for each phase of the project. The Regional Director, Area Manager and Chief Security Officer, will determine the allocation and source of funding for project

management activities. The Project Manager will keep the Area Office, Regional Security Officer, and Chief Security Officer fully informed of project status, problems, and issues.

7. **Controlled Access Area (CAA).** CAAs are specially-designated areas within a building or industrialized complex, such as a dam or powerplant, that contain highly-sensitive equipment, controls, or operations.

   A. At National Critical Infrastructure facilities, all primary and secondary operational control rooms, security control rooms, and Supervisory Control and Data Acquisition (SCADA) control rooms are automatically designated as CAAs.

   B. Any other CAAs, at all facility criticality levels, must be designated in a formal Decision Document. General access control areas (e.g., areas where access is controlled by a key card) are not CAAs unless they are designated as such in a formal Decision Document.

   C. Employees that have unescorted access to CAAs will have a position designation and background investigation as specified in Reclamation Manual D&S, *Personnel Security and Suitability* SLE 01-01, Appendix A. Designation of a CAA, as described in Paragraphs 7.A. and B., will require that existing position designations and access controls be evaluated and revised as necessary.

   D. Facility managers will implement physical and procedural access controls to limit unescorted access to CAAs to employees that have a successfully adjudicated background investigation at the appropriate level.

   E. Employees, contractors, and visitors who need to temporarily access a CAA, but do not have a successfully adjudicated background investigation at the appropriate level, will be escorted and monitored at all times by employees or contractors that have a successfully adjudicated background investigation at the appropriate level.

   F. Additional measures for the protection of Reclamation data and other IT resources will be applied in accordance with Reclamation Manual D&S *Reclamation Information Technology (IT) Security Program (ITSP): Physical Controls for IT* (IRM 08-08).

8. **Tours and Visitor Centers.** Tours and visitor centers often require unique security measures. The following requirements apply to Reclamation tours and visitor centers.

   A. Reclamation's Visitor Center Guidelines, issued by the Office of Policy and Program Services, contains a chapter on Tour and Visitor Center Security. This chapter must be

considered when designing 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. All non-public tours (such as school groups, technical groups, and international groups) must be scheduled with the facility in advance of the tour. The Regional Security Office or Area Officer Security Coordinator must also be notified of the tour, in advance.

C. The Office of International Affairs in Denver must be notified of all international visitors before visitors are allowed to participate on any non-public tours. International Affairs will coordinate with Reclamation's Law Enforcement Office to ensure each international visitor is properly vetted.

D. Tour guides and visitor center personnel must receive initial and biennial training in security awareness and tourism security and safety.

9. **Site Security Plans.** Site Security Plans will be developed by the Area Office for all facilities with a security criticality designation of Project Essential or higher. The plans will follow Reclamation's Site Security Plan template and will document security systems, procedures, and responsibilities for both normal operations and responses to security incidents. The plans will be used in conjunction with existing Standard Operating Plans, Emergency Action Plans, and other emergency occupancy and evacuation plans, as applicable. A copy of the plan and any revisions shall be transmitted to all appropriate offices, including the SSLE Security Office (84-45000).

10. **Guard Plans and Procedures.** The following 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 are employed to protect a facility: Standing Operating Procedures, Post Orders, Training Strategy, and Facility Defense Plan. A final copy of any security related procedures and contracts for NCI facilities and any revisions shall be transmitted upon approval to all appropriate offices, including the SSLE Security Office (84-45000). Guard plans and procedures shall be implemented before guards are deployed.

11. **Annual Reviews and Tests.** Area Office personnel must conduct annual reviews or tests of their Site Security Plans, access control measures, and security equipment and document the completion and results of the reviews and tests.

A. Site Security Plans will be reviewed at least annually to ensure procedures and contact information is accurate and complete.

B. Area Office personnel must conduct an annual check of electronic systems, such as detection, camera, and alarm systems, and physical security systems, such as barriers, fencing, locks, and gates, to ensure 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. However, recurring checks must be documented in the facility Standing Operating Procedures.

C. Area Office personnel must conduct an annual review of access control measures to ensure procedural compliance. This review will include a review of hard-key access controls, key inventories, and compliance with Personal Identity Verification card and temporary identification card procedures.