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 Security Policy

The goal of this Policy is to establish security requirements for the Bureau of Reclamation. The benefits of this Policy are the establishment of security program responsibilities including responsibilities associated with security risk assessments, collaboration, and decision making.

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 Policy.

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

Reclamation Manual

Policy

Subject: Security Program

Purpose: To establish security requirements for the Bureau of Reclamation. The benefits of this Policy are the establishment of security program responsibilities including responsibilities associated with security risk assessments and decisionmaking.

Authority: Reclamation Act of 1902, as amended and supplemented; Critical Infrastructure Protection Act of 2001; Homeland Security Act of 2002; Homeland Security Presidential Directives; Executive Orders 10450, 10577, 12958 as amended, and 12968; Public Law 100-235, Computer Security Act of 1987; Chapter 3 and 73 of Title 5, U.S. Code, Government Organizations and Employees; Title 5 Code of Federal Regulations (CFR) 731, 732, and 736; 32 CFR Parts 2001 and 2004; OMB Circular A-130, Appendix III; and Parts 441 through 446 of the Departmental Manual.

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

Contact: Security, Safety, and Law Enforcement Office (SSLE), 84-45000.

1. **Introduction.** Reclamation is responsible for the protection of an important part of the nation's critical infrastructure. A successful terrorist attack or other illegal activities could cause the disruption or failure of a critical water or hydropower facility, potentially leading to loss of life, national economic instability, loss of mission capability, and loss of public confidence in Reclamation's ability to carry out its mission.

2. **Program Purpose.** The purpose of Reclamation's Security Program is to provide protection of Reclamation's facilities, critical information, operations, plans and procedures, and more importantly, the employees, contractors, visitors, and public at or near its facilities. A key objective of the program is the reduction of security-related risks through a combination of preparedness, prevention, protection, and response. This is accomplished by prioritizing critical assets, identifying potential threats, assessing vulnerabilities and consequences, and mitigating unacceptable risks through integrated and cost effective security measures. Security measures may include facility fortification, surveillance and guard activities, effective security procedures, operational changes, and increased employee awareness.

3. **Scope.** This Policy and the supporting Directives and Standards apply to all Reclamation offices and all Reclamation-owned or -operated buildings, facilities, systems, and features, including those where operation and maintenance have been transferred to an operating entity.

4. **Responsibilities.**

A. **Commissioner and Deputy Commissioner.** The Commissioner and Deputy Commissioner, Policy, Administration and Budget (PAB) have executive oversight of Reclamation's Security Program. The Commissioner is the final approval authority for security-related Decision Documents related to National Critical Infrastructure and Major Mission Critical facilities. The Deputy Commissioner, PAB is the final approval authority for security-related Decision Documents related to Mission Critical facilities.

B. **Director, SSLE.** The Director, SSLE is responsible for overall development, implementation, and management of Reclamation's Security Program, including policy development, risk management, mitigation implementation, budgeting, and fund management. The Director, SSLE represents Reclamation on the Dam Sector Government Coordinating Council. The Director, SSLE is responsible for keeping the Commissioner and Deputy Commissioners adequately informed of security issues and decisions. The Director, SSLE is also responsible for ensuring that the Commissioner, Deputy Commissioners, and the Assistant Secretary – Water and Science (ASWS) are notified of any road closures, major security training exercises, and major changes in mission or public use, including changes in visitor tours. The Director, SSLE is the final approval authority for security-related Decision Documents related to Project Essential facilities.

C. **Security and Law Enforcement Advisory Board.** The advisory board is responsible for providing advice and support to the Director, SSLE in fulfilling his or her responsibilities as described above. Within this context, the advisory board will identify issues and make recommendations to the Director on security and law enforcement priorities, budgets, policies and business practices, program management, and options to best implement security and law enforcement functions throughout Reclamation. The advisory board will make recommendations on issues including, but not limited to, the scope and extent of the security and law enforcement programs, the evaluation of program goals and accomplishments, the interface and coordination of program elements and staff throughout Reclamation, determination of the threat environment and vulnerabilities for critical and essential facilities, and overall risk reduction strategies.

D. **Regional Directors and Managers.** Regional Directors, Area Managers, and Facility Managers are responsible for Reclamation project facilities and will ensure that offices, systems, and facilities are operated and maintained in accordance with applicable security Policy, Directives and Standards, procedures, and security-related Decision Documents. Regional Directors and Area Managers are responsible for keeping the Director, SSLE adequately informed of security issues and decisions; road restrictions, closures, and openings; major modifications to security equipment or procedures;

major security training exercises; requests to film movies and commercials on Reclamation property; major changes in security guard services; and major changes in mission or public use, including changes in visitor tours. Regional Directors and Area Managers are also responsible for ensuring that necessary actions to reduce risk are communicated to project beneficiaries and that these entities have an opportunity to participate in the development of risk reduction alternatives.

E. **Other Reclamation Directors.** Other Reclamation Directors will ensure that offices, systems, and facilities within their directorate are operated and maintained in accordance with applicable security Policy, Directives and Standards, and security-related Decision Documents. Reclamation Directors are responsible for keeping the Director, SSLE adequately informed of security issues and decisions.

F. **Chief Security Officer.** The Chief Security Officer is the principal staff person responsible for the formulation, coordination, management, operation, and oversight of all components of Reclamation's Security Program (see Sections 5A-5D). As part of the Facility Security component, the Chief Security Officer has oversight responsibility for all guard activities except weapons, explosives, and ammunition, which Reclamation's Law Enforcement Administrator has oversight responsibility for. The Chief Security Officer is responsible for development of security Policy, Directives and Standards, goals, procedures, and objectives. The Chief Security Officer will ensure appropriate outreach and coordination with other security offices and organizations such as the Department of the Interior's Office of Law Enforcement, Security, and Emergency Management; Department of Homeland Security; and other dam-sector agencies.

G. **Regional Security Officers (RSOs).** RSOs are responsible for implementation of Reclamation's Security Program and the coordination, management, and oversight of Security Program components and functions within their regions, including implementation of Reclamation Policy, Directives and Standards, and risk reduction strategies. RSOs are responsible for implementation of security awareness and Operations Security (OPSEC) programs throughout their respective regions.

H. **Area Office Security Coordinators.** Area Office Security Coordinators are responsible for implementation of Reclamation's Security Program and the coordination, management, and oversight of security functions within their area office, including implementation of Reclamation Policy, Directives and Standards, and risk reduction strategies. Area Office Security Coordinators are responsible for implementation of security awareness and OPSEC programs throughout their respective area offices, within the framework established by the RSO.

I. **Employees.** All Reclamation employees are responsible for:

(1) Integrating good security practices and procedures into all Reclamation operations and activities;

(2) Complying with all facility security measures and procedures to maximize the effectiveness of facility security systems and programs;

(3) Protecting sensitive information;

(4) Practicing security awareness and OPSEC, and promptly reporting security issues and suspicious incidents; and

(5) Monitoring and reporting changes that are needed in security posture based on changing project operations and conditions.

5. **Program Components.** Reclamation will maintain a risk-based Security Program consisting of the following major components:

A. **Personnel Security and Suitability.** Personnel Security and Suitability provides a basis for determining a person's suitability for Federal employment or work under a Federal contract, and where applicable, for determining whether a person is suitable to be placed in a Public Trust position, granted a National Security clearance, and/or issued a Personal Identity Verification Card.

B. **Information Security.** Information Security deals with the identification and safeguarding of National Security (classified) information and Sensitive but Unclassified For Official Use Only (FOUO) information.

C. **Facility Security.** Facility Security is concerned with the physical, technical, and procedural systems for protecting Reclamation's buildings and physical infrastructure, including guard functions. This includes the Security Risk Assessment process; supporting studies and development; design of physical security measures based on security risks; and implementation of physical security measures, plans, and procedures.

D. **Security Awareness/OPSEC.** This program component promotes the awareness of Reclamation employees and contractors to potential security threats, suspicious activities, and vulnerabilities in processes and routines. It includes periodic training on a Reclamation-wide, Regional, or Area Office basis on topics such as information security, reporting of suspicious incidents, the Emergency Notification System, and general security awareness. It also includes OPSEC which is an analytical process used to deny adversaries information concerning an agency's procedures and capabilities that could be useful in planning an attack.

E. **Related Program Areas.** In addition to the four major components listed above, there are three program areas that are closely related to the Security Program, but are not directly managed as part of the program. These include the Law Enforcement and Emergency Management programs, and the Information Technology (IT) Security program which is under the leadership of the Chief Information Officer.

6. **Program Staffing and Coordination.**

A. **Staffing.** Reclamation will provide technical security expertise and support for operations at all Reclamation levels through the hiring and training of experienced security personnel. Each Regional Office and NCI facility will have an experienced full-time Security Officer or Security Manager. Each area office will have an Area Office Security Coordinator, which may be a collateral duty position.

B. **Coordination.** Reclamation's Security Program can impact, or be impacted by, many other program areas and activities, such as dam safety, facility design and construction, operation and maintenance, safety, emergency management, human resources, land management, records management, and others. To ensure a safe and secure environment, Reclamation staff must make sure these program areas and activities are coordinated and integrated to the greatest extent possible.

C. **Operating Entities.** Where Reclamation has transferred the operation and maintenance of facilities to an operating entity, Reclamation will work closely with the operating entity on security-related activities such as security risk assessments, development of site security plans, exercising and testing of security plans and equipment, protection of sensitive information, and reporting of incidents. Decisions requiring action to reduce risk will be communicated to operating entities in a timely fashion. Whenever possible, operating entities will be informed on such decisions prior to the completion and approval of security-related Decision Documents.

7. **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. Facilities are placed into each category based on the following definitions and 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.

8. **Security Risk Assessments.** Reclamation will maintain a reiterative Security Risk Assessment (SRA) process for all NCI, MMC, MC, and PE facilities. The SRA process will have two primary components: the Comprehensive Security Review (CSR) and Periodic Security Review (PSR).

A. **Comprehensive Security Review (CSR).** A CSR will occur every six 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, Regional, and Area Offices. CSR findings, including any recommended mitigation actions, will be documented in a CSR Report. A Security Advisory Team (SAT) comprised of SSLE, Regional, and Area Office personnel will review and revise the CSR Report. All findings, including any recommended mitigation actions, will be documented in a formal Decision Document.

B. **Periodic Security Review (PSR).** A PSR will occur every six 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 combined PSR Report and Decision Document, using the PSR Report template provided by SSLE. Regional and Area Office personnel will review the PSR Report/Decision Document before routing for signatory approval. SSLE review is also recommended before routing for signatory approval.

C. **Risk Assessments by External Entities.** Many different entities, including the Department of Homeland Security, State Offices of Homeland Security, National Guard Bureau, 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 entities to conduct self-regulating 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 sent to the RSO for coordination and approval by the Chief Security Officer.

9. **Decisionmaking.**

A. **Documentation of SRA Decisions.** 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 the documentation will describe the decision, including the actions, timeframes, estimated cost, funding sources, and responsible office.

B. **Documentation of Supplementary Decisions.** Significant security decisions that are made outside the SRA process shall be documented in a supplementary Decision Document for signatory concurrence. This includes changes to previous SRA recommendations and decisions, and decisions that result in a significant change in security posture, such as changes in security guard strategies. The document will include a discussion of the issue and decision; associated actions, timeframes, responsibilities, estimated cost, and funding sources; and signatory concurrence lines. Approval of these supplementary decisions must be received by all decisionmakers before implementation may occur.

C. **Approval and Concurrence.** Security-related Decision Documents, including supplementary Decision Documents, will have signatory approval and concurrence as designated in the table below. An Approval Official may further delegate signatory approval for Decision Documents that do not contain any significant findings or recommendations. The Chief Security Officer will provide appropriate coordination with the Department of the Interior, Office of Law Enforcement, Security, and Emergency Management.

	Facility Criticality Level			
	NCI	**MMC**	**MC**	**PE**
ASWS	Concurrence	Conditional Concurrence[1]		
Commissioner	**Final Approval**	**Final Approval**	Conditional Concurrence[1]	
Deputy Commissioner	Approval	Approval	**Final Approval**	Conditional Concurrence[1]
Director, SSLE	Approval	Approval	Approval	**Final Approval**
Chief Security Officer	Approval	Approval	Approval	Approval
Regional Director	Approval	Approval	Approval	Approval
Area Manager	Approval	Approval	Approval	Approval

[1] Concurrence is required for any significant changes, including road restrictions, closures, or openings; major fortification activities, significant cost outlays, or major operational changes, such as significant guard force modification. The Final Approving official will determine if higher-level concurrence is required.

D. **Consultation with Project Beneficiaries.** Reclamation will consult with project beneficiaries on site security measures implemented after September 11, 2001.

(1) **Project Beneficiaries.** Project beneficiaries include water and power contractors, power marketing agencies, and operating entities (entities to which Reclamation has transferred facility operation and maintenance).

(2) **Notice.** Upon identifying a Reclamation facility for a site security measure, Reclamation will provide to the project beneficiaries written notice describing the need for the site security measure, describing the process for identifying and implementing the site security measure, and summarizing the administrative and legal requirements relating to the site security measure. For operating entities participating in a Comprehensive Security Review (CSR) or Periodic Security Review (PSR), the CSR or PSR process will meet this requirement. Information from the draft CSR report or PSR report may be provided to other project beneficiaries consistent with Reclamation's directives and standards for Identifying and Safeguarding For Official Use Only Information (SLE 02-01).

(3) **Consultation.** Reclamation will 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.

(4) **Response.** Before incurring costs related to increased levels of guards and patrols, training, patrols by local and tribal law enforcement entities, operation,

maintenance, and replacement of guard and response force equipment, and operation and maintenance of facility fortifications, Reclamation will consider cost containment measures recommended by a project beneficiary. Reclamation will provide to the project beneficiary a timely written response describing proposed actions to address the recommendations; and provide notice regarding the costs and status of such activities on a periodic basis.

(5) **Responsibility.** Notification, consultation, and response is the responsibility of the Regional and/or Area Office responsible for the facility. The Regional Security Officer, with the assistance of Reclamation's Security Office, will provide technical information and support regarding the need for the site security measure; planning, design, and construction; and estimated costs. Project beneficiaries who have elected to participate in the process of determining a risk reduction action are responsible for meeting the information security requirements according to Reclamation policy.

10. **Related Policies, Directives and Standards, and Guidelines.**

A. Department of the Interior policies related to security may be found in the Law Enforcement and Security Series of the Departmental Manual, Parts 441-446 (http://elips.doi.gov/app_dm).

B. Reclamation Directives and Standards for personnel security, information security, facility security, guards, law enforcement, and security-related components of emergency management are found in the Security and Law Enforcement section of the Reclamation Manual (http://www.usbr.gov/recman/DandS.html#sle).

C. Reclamation Policy and Directives and Standards for information technology security are found in the Information Resources Management section of the Reclamation Manual (http://www.usbr.gov/recman/policies.html#IRM and http://www.usbr.gov/recman/DandS.html#irm).

D. Annual security reporting requirements are found in the Directive and Standard on *Annual Reporting for Dam Safety, Security, and Related Operations* (http://www.usbr.gov/recman/fac/fac01-06.pdf).

E. Additional guidelines and information, such as the Security Risk Assessment Guidelines, Personal Identity Verification Handbook, Training Program for Reclamation's Security Professionals, and information on Security Awareness and OPSEC, are available from the Regional Security Officers or the Security Office (84-45000).