Reclamation Manual
Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

RECLAMATION
Managing Water in the West

FOR OFFICIAL USE ONLY

Physical Security Plan
XXXXXX Dam and Powerplant

FOR OFFICIAL USE ONLY

U.S. Department of the Interior
Bureau of Reclamation

March 15, 2012

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

Mission Statements

The mission of the Department of the Interior is to protect and provide access to our Nation's natural and cultural heritage and honor our trust responsibilities to Indian Tribes and our commitments to island communities.

The mission of the Bureau of Reclamation is to manage, develop, and protect water and related resources in an environmentally and economically sound manner in the interest of the American public.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

Physical Security Plan
XXXXXX Dam and Powerplant

In accordance with NERC CIP 006-3:
Cyber Security – Physical Security of Cyber Assets

FOR OFFICIAL USE ONLY

U.S. Department of the Interior
Bureau of Reclamation

Version 1.5
March 15, 2012

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

Contents

Page

1.2 Acronyms ... 1
2.1 Physical Security Perimeters ... 2
2.2 Identification of Physical Security Access Points ... 2
2.3 Monitoring ... 2
2.5 Access Authorization Management ... 4
2.6 Escort Procedures for Unauthorized Personnel ... 4
2.7 Physical Security Plan Revision Procedures ... 4
2.8 Physical Security Plan Annual Review ... 5
3. Protection of Physical Access Control Systems ... 5
4. Protection of Electronic Access Control Systems ... 5
6. Physical Access Monitoring ... 7
7. Logging Physical Access ... 7
8. Access Log Retention ... 7
9. Maintenance and Testing ... 8
9.1 Physical Security System Maintenance ... 8
9.2 Physical Security System Testing ... 8
9.3 Outage Records ... 8
Addendum A: Visitor Management Procedures ... 10
Addendum B: Access Device Loss Reporting Procedures ... 13
Addendum C: Inappropriate Access Attempt Procedures ... 15
Addendum D: Access Authorization Management Procedures ... 17
Addendum E: Annual Review of Physical Security Plan ... 21
Addendum F: Security System Management Procedures ... 23
Addendum G: Physical Security Perimeter (PSP) Inventory and Descriptions ... 25

FOR OFFICIAL USE ONLY

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

Document History

Version No.	Date	Revision Description
1.1	07/14/2009	Original issue
1.2	08/05/2009	Integrated review comments
1.3	08/11/2009	General Revisions
1.4	1/20/2011	Revised to reflect Version 3
1.5	3/15/2012	Changed CIO to DIRO

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

1. Introduction

1.1 Purpose and Scope

This Physical Security Plan addresses compliance for the Bureau of Reclamation's (Reclamation) XXXXX XXXXX Region, XXXXXX Dam and Powerplant (XXXXXX) with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) 006-3. The following are the Critical Assets (CA) included in this Physical Security Plan for XXXXXX as determined by the Reclamation Power Resources Office on December 20, 2010, in accordance with the requirements defined in CIP 002-3.

Critical Asset	Critical Functions Performed
XXXXXX Control Center	Controls Critical Assets at multiple Bulk Power System (BPS) facilities.
XXXXXX Powerplant	Essential to the system due to size, 2,000+ megawatts, and role as a blackstart generator critical to the BPS restoration plan.
XXXXXX Powerplant 230-kilovolt "Busbar" (BCP)	Transmission path(s) for blackstart generation critical to the BPS restoration plan.

1.2 Acronyms

BPS	Bulk Power System
CA	Critical Assets
CCA	Critical Cyber Assets
CIP	Critical Infrastructure Protection
CO	Contracting Officer
COR/COTR	Contracting Officer's Representative
EACSS	Electronic Access Control Security System
ESP	Electronic Security Perimeters
ISS	Integrated Security System
NCCA	Non-Critical Cyber Assets
NERC	North American Electric Reliability Corporation
PIV	Personal Identity Verification
PM	Project Manager
PSP	Physical Security Perimeter
RESC	Reclamation Enterprise Services Center
Reclamation	Bureau of Reclamation

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 1

FOR OFFICIAL USE ONLY

2. Requirements

2.1 Physical Security Perimeters
(NERC CIP 006-3, R1.1)

All Cyber Assets that are essential to the reliable operation of CAs at XXXXXX Dam and Powerplant are designated as Critical Cyber Assets (CCA) and have been identified in accordance with CIP 002. The CCAs associated with the operation of XXXXXX are contained within logical borders identified as Electronic Security Perimeters (ESP) to which physical access is controlled through Physical Security Perimeters (PSP). The PSPs at XXXXXX have been established after the identification of the CCAs and designation of their related ESP by the Reclamation Director of Information Resources. Representatives of Security, Safety, and Law Enforcement and the Regional Security Office conducted security assessments of the ESPs to determine the PSPs and measures that will be required for compliance. The results of the assessments and the description of the PSPs at XXXXXX are included in the *Physical Security Perimeter Inventory and Descriptions* located in Addendum G. The inventory identifies each PSP at XXXXXX and details compliance actions.

2.2 Identification of Physical Security Access Points
(NERC CIP 006-3, R1.2)

All physical access entry points into each PSP are controlled by card key systems, special locks, security personnel, or a combination of these systems. The specific measures to control entry at each access point are detailed in Section 3 of the PSP (Addendum G).

2.3 Monitoring
(NERC CIP 006-3, R1.3)

All XXXXXX PSP access points are electronically monitored by the XXXXXX Dam Security Control Center on a 24/7 basis. In specific instances, the electronic monitoring may be supplemented by direct monitoring performed by onsite personnel. The specific measures to monitor entry activity at each access point are detailed in Section 4 of the PSP (Addendum G).

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

2.4 Physical Access Controls
(NERC CIP 006-3, R1.4)

2.4.1 Visitor Management
(NERC CIP 006-3, R1.6)

All employees, contractors, operating partners, and visitors who have not previously been issued specific PSP access authorization must be continuously escorted by an individual with specific PSP access rights when accessing the PSP. Access activity will be manually recorded by authorized personnel. Logs include entries for: the PSP accessed, name, name of escort, time in/out, and purpose of visit.

Addendum A contains Visitor Management Procedures and a sample *Access Log*.

2.4.2 Response to Loss
Individuals are required to immediately report the loss or theft of a PSP access control card to their immediate supervisor and the XXXXXX Dam Security Department. The XXXXXX Dam Security Department will initiate termination of all card access control rights of the individual whose card has been reported missing. If the PSP access control card is a USAccess card issued by Reclamation, the loss must also be reported to the Reclamation Enterprise Services Center (RESC) at 303-445-3357 in accordance with Reclamation's *Standard Procedures for Issuance and Management of Personal Identity Verification Cards*.

Individuals are required to immediately report the loss or theft of PSP access keys to their immediate supervisor and the XXXXXX Dam Security Department. The Facility Security Manager will initiate appropriate action to ensure the integrity of the PSP key locking system is not compromised.

Replacement access devices, if required, will be issued in accordance with Section 2.5 below.

Addendum B contains the procedures to report and document losses and a sample *Access Device Loss Report*.

2.4.3 Prohibition of Inappropriate Use of Physical Access Controls
Individuals authorized for unescorted access to a PSP receive training in accordance with CIP-004. Included in the training is awareness of the proper use of physical and electronic access controls. In addition, signage advising the prohibition of unauthorized access is posted at PSP access points.

FOR OFFICIAL USE ONLY

Procedures to address inappropriate use and unauthorized access attempts as registered by the card access control system or, in the case of the improper use of keys or forced entry, as registered by the intrusion detection system, include response efforts ranging from internal management and disciplinary actions to immediate investigation efforts by the Facility Security Manager. Addendum C contains these procedures and a sample *Access Attempt Report*.

2.5 Access Authorization Management

(NERC CIP 006-2, R1.5)

All specific PSP access authorization requests must be completed in accordance with the access authorization management procedures included in Addendum D. A completed *Access Authorization Request Form* is then transmitted to the Security Department for access control system programming or key issuance. Access authorizations are logged by the card access system, including card holder identity, programmer identity, authorization level details, time, and date. Key issuance activity is manually logged including key holder identity, issuer identity, key identity, time, and date. Both electronic and manual logs are retained for a minimum of 1 year from date of issuance.

When access has been granted, the above information will be forwarded to the local access control individual for entry and tracking into the authorized access list as defined by CIP 004-3 R4.

2.6 Escort Procedures for Unauthorized Personnel

(NERC CIP 006-2, R1.6)

All employees, contractors, operating partners, and visitors who have not previously been issued specific PSP access authorization will be continuously escorted by an individual with specific PSP access rights when accessing a PSP. Access activity will be manually recorded by authorized personnel. Logs include entries for: the PSP accessed, name of visitor, name of escort, time in/out, and purpose of visit.

Addendum A contains Visitor Management Procedures and a sample *Access Log*.

2.7 Physical Security Plan Revision Procedures

(NERC CIP 006-2, R1.7)

This Physical Security Plan will be revised within 30 calendar days of the completion of any physical security system redesign or reconfiguration, including

but not limited to the addition or removal of access points into a PSP, physical access controls, monitoring controls, or logging controls.

The Facility Security Manager, in collaboration with the Facility IT Security Manager, is responsible for all Physical Security Plan revisions.

Revision actions will be noted in the *Document History* (page v), and the Physical Security Plan will be reissued.

2.8 Physical Security Plan Annual Review
(NERC CIP 006-2, R1.8)

A review of the Physical Security Plan will be conducted annually by the Facility Security Manager, in collaboration with the Facility IT Security Manager. These annual reviews will be noted in Addendum E, and any resultant revisions to the Physical Security Plan will be accomplished in accordance with Section 2.7 above.

3. Protection of Physical Access Control Systems
(NERC CIP 006-3, R2)

Non-critical Cyber Assets that comprise the physical access control system are protected from unauthorized physical access and feature physical access controls as specified in NERC CIP 006-3, R4 and R5. Although a PSP is not required for these assets, details regarding the non-critical Cyber Assets and physical access features are included in the *Physical Security Perimeter Inventory and Descriptions* in Addendum G to maintain consistency.

Non-critical Cyber Assets that comprise the Electronic Access Control Security System (EACSS) are within an ESP and a related PSP, and are afforded all the protective measures specified for PSPs and ESPs. Details of the PSP for this system are included in the *Physical Security Perimeter Inventory and Descriptions* in Addendum G.

4. Protection of Electronic Access Control Systems
(NERC CIP 006-3, R3)

The non-critical Cyber Assets used in the access control and/or monitoring of the ESP shall reside within an identified PSP. All ESP components meet this requirement. Details regarding these non-critical Cyber Assets and surrounding

FOR OFFICIAL USE ONLY

PSP are included in the *Physical Security Perimeter Inventory and Descriptions* in Addendum G.

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 6

FOR OFFICIAL USE ONLY

5. Physical Access Controls
(NERC CIP 006-3, R4)

The physical access methods employed at the XXXXXX Dam include card key, special locks, and security personnel. The specific method(s) for physical security access at each PSP access point are detailed in Section 3 of the *Physical Security Perimeter Inventory and Descriptions* I Addendum G.

6. Physical Access Monitoring
(NERC CIP 006-3, R5)

All intrusion detection, closed circuit television surveillance, and card access control systems are monitored on a 24/7 basis at the XXXXXX Dam Security Control Center. Upon receipt of an indication of an unauthorized intrusion event, the Security Control Center operator will immediately notify security or police personnel to initiate investigation efforts.

Procedures to address inappropriate use and unauthorized access attempts as registered by the card access control system or, in the case of the improper use of keys or forced entry as registered by the intrusion detection system, include response efforts ranging from internal management and disciplinary actions to immediate investigation efforts by the Facility Security Manager. Addendum C contains these procedures and a sample *Access Attempt Report*.

7. Logging Physical Access
(NERC CIP 006-3, R6)

Access event logging uniquely identifies individuals and time of access on a 24/7 basis. The logging methods for the physical access controls at each PSP access point are detailed in Section 6 of the *Physical Security Perimeter Inventory and Descriptions* in Addendum G.

8. Access Log Retention
(NERC CIP 006-3, R7)

Physical access logs for both card access, intrusion detection activity, and visitor access logs are retained at the XXXXXX Dam Security Department for a minimum of 1 year.

Logs relating to reportable incidents will be retained in hard copy for a period of 3 years.

FOR OFFICIAL USE ONLY

The Facility Security Manager is responsible for access log retention.

9. Maintenance and Testing
(NERC CIP 006-3, R8)

9.1 Physical Security System Maintenance

All physical security system access control devices will be maintained in accordance with the manufacturer's recommendations and specifications. Maintenance actions will be recorded and records will be retained for the life of the system.

The XXXXXX Integrated Security System (ISS) administrator is responsible for the establishment and coordination of all maintenance activities and retention of maintenance records in accordance with procedures in Addendum F.

9.2 Physical Security System Testing

All physical security system access control devices will be tested to confirm proper operation on a cycle not to exceed 3 years.

Testing actions will be recorded and test records will be retained for the life of the system.

The XXXXXX ISS administrator is responsible for the establishment and coordination of all testing activities and retention of testing records in accordance with procedures in Addendum F.

9.3 Outage Records

Outage events regarding access controls, logging, and monitoring shall be recorded and retained for a minimum of 1 calendar year from the date of the outage.

The XXXXXX ISS administrator is responsible for the documentation of outage events in accordance with procedures in Addendum F.

FOR OFFICIAL USE ONLY

10. Approvals
(NERC CIP 006-3, R1)

Our signatures below signify approval and acceptance of this Physical Security Plan.

_____

XXXXX X, XXXXXXX — Date
Security Manager, XXXXXX Dam

_____

XXXXX X, XXXXXXX — Date
Facility Manager, XXXXXX Dam

_____

XXXXX X, XXXXXXX — Date
Area Manager, XXXXXX Dam

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Addendum A: Visitor Management Procedures

1. Purpose

This defines the procedures that are required to provide for secure access to PSPs by employees, contractors, operating partners, and visitors who have not been previously issued specific PSP access authorization.

2. Procedures

a. Continuous Escort

While accessing a PSP, all employees, contractors, and visitors without access rights must be continuously escorted by an individual who has access rights to the specific PSP. Contractors with specific PSP access rights may not escort other contractors, operating partners, visitors, or employees without access rights.

b. Access Event Logging

All PSP access activity by persons without access rights must be recorded by an individual who has access rights to the specific PSP. Contractors with specific PSP access rights may not record access activity by other contractors, operating partners, visitors, or employees without access rights.

c. Log Details

An *Access Log* will be available for each PSP and will include entries for:

(1) Date
(2) Name
(3) Escort name
(4) Time in/out
(5) Purpose of visit

A sample *Access Log* follows these procedures.

d. Log Management

Logs will be collected from each PSP on a semi-annual basis and retained for 1 year except those logs that may involve inappropriate access events. These must be retained for 3 years.

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 10

3. Responsibility

The Facility Security Manager is responsible for placing, collection, and retention of the *Access Logs*.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

ACCESS LOG							
Facility:			PSP:				
Date:	To be completed by escort						
	Name (print)	Name (sign)	Name (print)	Name (sign)	In	Out	Purpose of visit

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 12

Addendum B: Access Device Loss Reporting Procedures

1. Purpose

This defines the procedures that are required to report and manage the loss of a PSP access control card or key.

2. Procedures

a. Card/Key Holder Report

The person incurring the loss must complete Section 1 of an *Access Device Loss Report*, complete with a statement to include sufficient information regarding the loss so that the Facility Security Manager can determine if a compromise has occurred. If the lost access device is an access control card, the loss must also be reported to the RESC. The report is then forwarded to the XXXXXX Dam Security Department.

A sample *Access Device Loss Report* follows these procedures.

b. Security Department Report

The Security Department representative processing the report must complete Section 2 of the Access Device Loss Report and corresponding Section 6 of the original *Access Authorization Request Form* (Addendum D) and forward the *Access Device Loss Report* to the Facility Security Manager.

c. Facility Security Manager

The Facility Security Manager will complete Section 3 of the Access Device Loss Report to confirm his/her review of it and determination if a potential or actual compromise occurred and any follow up actions.

d. Report Management

Reports will be retained for 1 year, except those reports that may involve compromise events. Those reports will be retained for 3 years.

3. Responsibility

The Facility Security Manager is responsible for retention of the *Access Device Loss Report*.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

ACCESS DEVICE LOSS REPORT	
Section 1, To be completed by card/key holder	
Facility:	
Date of loss:	
Date of report:	
Card/key holder statement:	
If needed use reverse side	
Reported to RESC (Reclamation USAccess cards only) Tel. 303-445-3357	
Reported to Security Department	Reported to supervisor
Name (print)	Name (sign)

Section 2, To be completed by the Security Department		
Report received date:		
Original Access Authorization Request Form completed (section 6)		
New card/key(s) issued	Yes	No
Comments:		
If needed use reverse side		
Name (print)	Name (sign)	

Section 3, To be completed by the Security Manager	
Loss incident review and any comments to include followup recommendations	
If needed use reverse side	
Name (sign)	Date

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 14

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

Addendum C: Inappropriate Access Attempt Procedures

1. Purpose

This defines the procedures that are required to manage and document the inappropriate use of Physical Access Controls.

2. Procedures

a. Attempt Discovery

Inappropriate PSP access attempt activity must be reported through the Physical Security System, ECASS, or by visual contact. Upon receipt of an inappropriate PSP access attempt, the Security Control Center Operator will immediately determine the response action and complete Section 1 of the *Access Attempt Report*.

A sample *Access Attempt Report* follows these procedures.

b. Response Action

The investigating officer will respond to the PSP location and conduct an assessment to determine the cause of the incident. The officer will document his/her findings in Section 2 of the *Access Attempt Report*.

c. Management Review

The incident report and any follow-up investigation actions will be reviewed by the Facility Security Manager to determine if further action is warranted.

d. Report Management

Reports will be retained for 1 year, except those reports that may involve inappropriate access events. These will be retained for 3 years.

3. Responsibility

The Facility Security Manager is responsible for oversight of this procedure.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

ACCESS ATTEMPT REPORT	
Section 1, To be completed by the Security Control Center Operator	
Facility:	Date of report:
PSP identification and No.:	
Date of attempt:	Time of attempt:
Type of attempt:	
Card reader	Reader ID:
Access control event transaction No.	
Intrusion detection system	Point No.:
Intrusion detection system event transaction No:	
Visual observation	
Reported by:	
Name (print)	Telephone
Response action:	
If needed use reverse side	
Report prepared by:	
Name (print)	Name (sign)

Section 2, To be completed by the Investigating Officer	
Investigation action:	
If needed use reverse side	
Investigation report prepared by:	
Name (print)	Name (sign)

Section 3, To be completed by the Facility Security Manager	
Investigation report reviewed by:	
Name (print)	Name (sign)
Title:	Date:
Comments:	
If needed use reverse side	

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 16

Addendum D: Access Authorization Management Procedures

1. Purpose

This defines the procedures that are required to manage the PSP access authorization process.

2. Procedures

a. Request Action

The person requesting access to a PSP must complete Section 1 of the *Access Authorization Request Form*, including all information. Contractors requesting PSP access must also complete Section 2. The form must then be submitted to the requesting employee's supervisor or requesting Contracting Officer's Representative/Contracting Officer/Project Manager (COR/CO/PM) for approval.

A sample *Access Authorization Request Form* follows these procedures.

b. Supervisory Approval

The supervisor or COR/CO/PM will review the request and, if appropriate, sign and forward to the local access control individual.

c. CIP-004 Requirements Completion Verification

The local access control individual will confirm in Section 4 that the requestor has completed the Personnel Risk Assessment and cyber security training in accordance with CIP-004 and forward the request to the PSP manager.

d. PSP Manager Action

The specific PSP Manager will review the request to determine if access is warranted and signify approval.

e. Issuance

The approved request form is transmitted to the XXXXXX Dam Security Department for issue of the access device. Details regarding the device will be recorded in Section 6, and the form will be filed at the Security Department. A copy of the request form is to be forwarded to local access control individual.

f. Surrender

When the PSP access device is no longer needed, or access rights are revoked, the XXXXXX Dam Security Department will complete Section 7, including requestor information. A copy of the request form is to be forwarded to the local access control individual.

g. Form Management

Access Authorization Request Forms will be retained at the XXXXXX Dam Security Department until the individual's access rights are surrendered or revoked. Forms containing surrender or revocation actions will be retained for 3 years from the date of the action.

3. Responsibility

The Facility Security Manager is responsible for oversight of this procedure.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

ACCESS AUTHORIZATION REQUEST FORM			
Section 1, To be completed by requestor			
Facility:			
List PSP request(s):			
If needed, list additional PSP access requests on back			
List reason for access:			
If needed, list additional reasons for access on back			
Last name:		First name:	MI:
Status:	Employee	Operating partner	Contractor
Title:			
Work location:			
Telephone:		E-Mail:	
Signature:		Date:	

Section 2, To be completed by contractor requestor	
Company:	
Contract No.:	Contract completion date:

Section 3, Submit this form to your Supervisor or COR/CO/PM for approval		
For employees and operating partners		
Supervisor name (print)	Supervisor name (sign)	Date:
Supervisor title:	Supervisor phone:	
For contractors		
COR/CO/PM name (print)	COR/CO/PM name (sign)	Date:

Section 4, Submit this form to the local access control individual for verification		
Personnel risk assessment completed:	Yes, Date:	No
Cyber security training completed:	Yes, Date:	No
Custodian name (print)	Custodian name (sign)	Date:

Section 5, Submit this form to the PSP Manager for approval		
Manager name (print)	Manager name (sign)	Date:
Manager title:		

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 19

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

ACCESS AUTHORIZATION REQUEST FORM (continued)		
Section 6, Issuance		
PIV verified	Copy for CIP 004-2, R4	
Existing access card programmed	Card No.:	
New access card issued	Card No.:	
Keys issued	Key Nos.:	
Issuer name (print)	Issuer name (sign)	Date:
Issuer title:		

Section 7, To be completed when PSP access is surrendered or revoked		
Requested by (print)	Signature:	Date:
Title:		
Reason for surrender/revocation:		
If needed use reverse side		
Access card deprogrammed	Date:	
Access card retrieved	Date:	
Keys returned	Date:	
Copy for CIP 004-2, R4	Date:	
Revoked by (print)	Signature:	Date:
Title:		

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 20

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

FOR OFFICIAL USE ONLY

Addendum E: Annual Review of Physical Security Plan

Reviewer	Title	Date	Action

Addendum F: Security System Management Procedures

1. Purpose

This defines the procedures that are required to manage the physical security and ECASS systems and document related maintenance, testing, and outage activity.

2. Procedures

a. System Maintenance

Maintenance of all system components will be performed in accordance with the manufacturer's recommendations and specifications. The XXXXXX ISS administrator will establish a maintenance inventory record to include the device identification, manufacturer, installation location, maintenance schedule, and the date when the last maintenance was performed.

The ISS administrator will retain this inventory for the life of the system.

b. System Testing

All security system devices will be tested to confirm proper operation on a cycle not to exceed 3 years or the manufacturer's recommendations. The XXXXXX ISS administrator will establish a testing inventory record to include the device identification, manufacturer, installation location, test schedule, and the date when the last test was performed. This inventory can be combined with the maintenance inventory in 2.a. above.

The ISS administrator will retain this inventory for the life of the system.

c. Outage Records

The ISS administrator will establish a log to record outage events to include date, device(s) or system outage description, restoration action, and time.

The ISS administrator will retain this log for minimum of 1 year from the date of the outage.

3. Responsibility

The XXXXXX ISS administrator is responsible for compliance with these procedures.

FOR OFFICIAL USE ONLY

Addendum G: Physical Security Perimeter (PSP) Inventory and Descriptions

PSP Description Instructions and Inventory	
Facility: XXXXXX Dam and Powerplant	**Date:** 07/14/2009 (original)
List each PSP on the following inventory list and complete and attach a separate description form following the instructions in each section. Include the date and indicate if the form is the original or a revision.	
PSP No.	**PSP Title**
1	Powerplant Control Center

FOR OFFICIAL USE ONLY

Facility: XXXXXX Dam and Powerplant	**Date:** 07/14/2009 (original)
Critical Asset: Control Center	
Physical Security Perimeter: Powerplant Control Center	**PSP No.** 0001
***1. Electronic Security Perimeter (ESP) Description:* Include the description of the ESP, as well as details of the Critical Cyber Assets (CCAs) located within the ESP. Refer to Reclamation's documentation for CIP 002 for information concerning CCAs and CIP 005 for information concerning ESPs to be included in this section.**	
The Control Center has the following CCAs: Cisco switches, (8) view nodes, and map board. These CCAs are enclosed in one ESP within the control center perimeter.	
***2. PSP Description:* Identify the physical characteristics of the PSP. For general information, refer to Section 2.1, Physical Security Perimeters, in the body of the Physical Security Plan.**	
The ESP is entirely located within the Control Center, which has six-sided perimeter consisting of side walls, floor, and ceiling.	
***3. Access Points:* Identify all physical access points into each PSP and measures to control entry into the points (CIP 006-2 R1.2).**	
There are three active doors where access is controlled by card readers and unescorted access limited to authorized persons.	
4. Monitoring Physical Access: List the processes, tools, and procedures used to monitor physical access to the PSPs (CIP 006-2 R1.3).	
Unauthorized access activity is registered by an IDS consisting of balanced magnetic switches installed on all doors. The Intrusion Detection System is monitored on a 24/7 basis at the XXXXXX Dam Security Control Center. Visual monitoring of physical access points is also accomplished by the control center personnel who are onsite on a 24/7 basis. XXXXXX Dam Security Officers are immediately notified to respond to investigate unauthorized access events.	
***5. Management of Physical Access:* List the operational and procedural controls used to manage physical access to the PSPs (CIP 006-2 R4).**	
Access to all active doors is controlled by card key, which is centrally managed at the XXXXXX Dam Security Department. Only authorized persons have card access rights.	
***6. Description of Logging Methods:* List access activity logging methods (CIP 006-2 R6).**	
All card reader transactions are individually electronically logged. Main entrance access activity is under video surveillance and recorded. Those individuals without authorized access are actively escorted by an authorized individual. All visitor entry activity not recorded by a card reader transaction or the video system is manually logged by the control center staff.	

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 26

FOR OFFICIAL USE ONLY

Facility: XXXXXX Dam and Powerplant	
Critical Asset:	
Physical Security Perimeter:	**PSP No.** 0002
1. Electronic Security Perimeter (ESP) Description: **Include the description of the ESP, as well as details of the CCAs located within the ESP. Refer to Reclamation's documentation for CIP 002 for information concerning CCAs and CIP 005 for information concerning ESPs to be included in this section.**	
2. PSP Description: Identify the physical characteristics of the PSP. For general information, refer to Section 2.1, Physical Security Perimeters, in the body of the Physical Security Plan.	
3. Access Points: **Identify all physical access points into each PSP and measures to control entry into the points (CIP 006-2 R1.2).**	
4. Monitoring Physical Access: **List the processes, tools, and procedures used to monitor physical access to the PSPs (CIP 006-2 R1.3).**	
5. Management of Physical Access: **List the operational and procedural controls used to manage physical access to the PSPs (CIP 006-2 R4).**	
6. Description of Logging Methods: **List access activity logging methods (CIP 006-2 R6).**	

FOR OFFICIAL USE ONLY

Version 1.4
XXXXXX Dam and Powerplant, Page 27