Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

Physical Security Plan: Instructions

As part of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance requirements a physical security plan is required for each Bureau of Reclamation (Reclamation) facility designated as a Critical Asset (CA). For those facilities not designated as CAs but requiring protection due to interconnections of Critical Cyber Assets (CCA) with designated CA facilities it is recommended a separate Physical Security Plan be prepared for the non-CA facility.

This document can stand alone or be included as an appendix to an existing Site Security Plan. This determination should be made at the local level. When incorporating this document into an existing plan or procedure (SOP, Site Security Plan, etc.), it is recommended that the attached Physical Security Plan template be completed in its entirety and then included as an appendix. This will ensure consistency across Reclamation when it comes to documentation of compliance with this requirement.

The template found in Appendix A is designed to mirror the requirements detailed in CIP 006. When complete, the physical security plan must document Reclamation's compliance with the requirements of this standard. This plan is designed to be self-contained. All information about the protection measures for the individual PSP are contained within the body of the plan and the several addendums. Where possible, it is encouraged that local offices use existing procedures to ensure the processes are workable on a local level.

As with all the CIPs, there is considerable interconnection between the requirements; they all build upon each other. It is recommended you familiarize yourself with the other requirements. Prior to completion of the plan, the following steps must be accomplished.

1. Identification of CAs (CIP 002) is the responsibility of the Power Resources Office (PRO)

2. Identification of CCA (CIP 002) is the responsibility of the area and facility managers as supported by policy and guidance produced by the CIO (CIO)

3. Identification of Electronic Security Perimeters (ESP) (CIP 005) is the responsibility of the Area and Facility Managers as supported by policy and guidance produced by the CIO (CIO)

4. Identification of Physical Security Perimeters (PSP) (CIP 006)
    a. Recommend be done in conjunction with the identification of ESP
    b. Responsibility of Regional Security Officer, in conjunction with SSLE

There are several options when identifying the Physical Security Perimeters. Where feasible, a large all encompassing PSP can be identified. This may be an entire plant, using the six walls of the plant as the boundaries. In other cases, several PSP may be

needed to adequately protect the CCA, as well as ensure uninterrupted operations of the facility. When using smaller PSP they may be cabinets, smaller rooms, or other six-wall boundary. Each facility will have a different approach based on local needs. This template is designed to address both of these options. As part of the identification process, each PSP must be given a name and/or unique identifier. This will allow for easy reference as you move through the process.

This Physical Security Plan is required to document the results and security measures associated with the PSP. Detailed information for the actual physical protections used in the PSP is not included in the standard. For additional information on this matter, consult with your local Regional Security Officer.

The following information is provided for your use when completing the PSP. General and specific information must be included as part of the plan. Details of procedures and access control measures that apply to all PSP must be in the body of the plan; information specific to a single PSP must be detailed in Addendum G. Specific information on each PSP and its security components must be detailed in the PSP inventory (Addendum G). The PSP inventory must contain the necessary detailed information needed to ensure compliance.

The following information is denoted by titles. Titles correspond to the template. The language included in the template is primarily aimed at large facilities with Electronic Access Control Systems. For smaller facilities with less extensive security systems considerable revision may be required. The instructions are designed to offer alternatives when rewriting. However, local procedures must be taken into consideration and incorporated when developing the plan.

Document History:

This section details all changes made to the document over time. Recommend starting with Version 1. The date must be the date approved by the approving official. The approving official is normally the area manager; however, each facility must determine the appropriate senior management approvals.

1 Introduction:

No text needed.

1.1 Purpose and Scope:

This section details specific information for the specific CA. Details must include the region and facility name. The specific CA information can be found in the PRO annual memorandum used to document Reclamation's CA list. This section is designed to show the initial building block in the process. Specific CCA are to be listed as part of Addendum G that details the CCA protected by each PSP. Please find additional information below under Addendum G.

1.2 Acronyms:

This section details the acronyms currently in use in the template. Please add or delete as necessary.

2 Requirements:

No text needed.

2.1 Physical Security Perimeters:

This section includes general information detailing the process for identification of CCA, ESP, and PSP. The name of the specific facility being referenced must be included throughout the section. Detailed information on the PSP must be located in Addendum G. Language in the template applies to all facilities.

2.2 Identification of Physical Security Access Points:

Detail the access points to each PSP, as well as the access control measures used for each access point. Language in the template can be used for those facilities with an electronic access control system.

Those facilities without electronic access control systems will need to develop a detailed paper based process to describe all entrances and track access for each PSP. Egress is optional, but recommended for those facilities using a paper process. A sample access log is included in Addendum A. All logs detailing access to the system must include at a minimum: the PSP accessed; the name of person accessing the PSP; time in/out, and the purpose of visit.

Measures specific to each PSP are also defined in the PSP inventory (Addendum G).

For those facilities where electronic access control is not used, the measures used to protect the physical security access points must be detailed here. If a key system is used, this could be as simple as detailing the type of lock system and how it prevents access by unauthorized individuals.

2.3 Monitoring:

Detail the processes, tools, and procedures used to monitor physical access to the PSP. Language in the template can be used for those facilities with an electronic access control system. Where an electronic monitoring system does not exist, alternate manual measures must be clearly defined. Alternates include: physical observation (by authorized employee), electronic key card access logs, or any other method used to monitor and control access.

Measures specific to each PSP are also defined in the PSP inventory (Addendum G).

For those facilities where electronic access control is not used, the measures used to monitor physical access to the PSP must be detailed here.

2.4 Physical Access Controls:

No text needed.

2.4.1 Visitor Management:

Detail the access control measures used to manage all visitors (any individual, including employees without authorized access to the specific PSP) to the PSP. A sample visitor log and visitor management procedures can be found in Addendum A.

Generally visitor management is done via a paper process and is manually recorded, even for those facilities with an electronic access control system. Language in the template can be used for all facilities.

2.4.2 Response to Loss:

Detail the reporting procedures for loss of any access control device (card key or physical key). Procedures must include reporting requirements to whoever in the plant can immediately revoke access to prevent unauthorized use of the access control device or compromise of the CCA. Language in the template must be adapted for all facilities with specific points of contact.

The term Dam Security Manager is used throughout the template to denote the suggested position responsible for a variety of specific tasks. In some facilities this position may be known as the Physical Security Specialist, Collateral Duty Security Officer, etc. While the general recommendation is to have the local security person responsible for the physical security plan and associated duties, each facility must designate the position best suited to fulfill the requirements. Once designated, the position must be clearly communicated to all involved in the process. If warranted, this position can be designated in writing.

Specific procedures for reporting and documentation are provided in Addendum B. See below for additional information.

2.4.3 Prohibition of Inappropriate Use of Physical Access Controls:

Detail the response for any inappropriate use or unauthorized access attempt. Response must include how the inappropriate use or unauthorized access attempts are identified, as

well as who is responsible for investigating said attempts. Language in the template can be used for those facilities with an electronic access control system. Where an electronic monitoring system does not exist, alternate measures must be developed and included.

The training materials are being developed separately. Once details of how that will be accomplished are known, the template will be updated.

For those facilities where electronic access control is not used, the measures used to identify inappropriate use of access controls must be detailed here.

Standard language for signage will be developed and inserted when complete.

2.5 Access Authorization Management:

Detail the process for approval of unescorted physical access to the PSP. Process must follow the form in Addendum D. Procedures include identification of who (by position) has the authority to actually grant access (issue keys; program card keys) to the specific PSP. Language in the template can be used for all facilities. A draft procedure and form for access management is included in Addendum D. See below for additional information.

A sample visitor log and visitor management procedures can be found in Addendum A. Additional information on visitor management is located above.

2.6 Escort Procedures for Unauthorized Personnel:

In addition to the logging requirements for visitors (anyone without authorized PSP access) noted above, visitors must also be continuously escorted while accessing or inside the PSP. This section reiterates that requirement. If specific local escort procedures are used, insert here. Language in the template can be used for all facilities.

A sample visitor log and visitor management procedures can be found in Addendum A. Additional information on visitor management is located above.

2.7 / 2.8 Physical Security Plan Revision Procedures / Physical Security Plan Annual Review:

Detail the revision requirements as defined in the standards. Language in the template can be used for all facilities. This section clearly identifies the position responsible for maintaining the plan, including all required reviews and revisions. Language in the template can be used for all facilities if specific points of contact are incorporated.

3 Protection of Physical Access Control Systems:

This section only applies to those facilities that are using electronic access control systems, to authorize and log access. Language in the template must be used for all facilities with electronic access controls. Details of the protection measures should be documented in the PSP inventory (Addendum G).

If there is no electronic Physical Access Control System used at a facility then the following language must be inserted: No electronic physical access controls are employed in the protection of the PSP at XXX facility. This section is not applicable.

4 Protection of Electronic Access Control Systems:

This section reiterates compliance with the requirement to ensure that all cyber assets associated with ESP access and monitoring reside within a PSP. Language in the template can be used for all facilities. Details of the protection measures must be documented in the PSP inventory (Addendum G).

5 Physical Access Controls:

Detail the operational and procedural controls to manage physical access at all access points to the PSP 24/7. One of the following methods must be used: card key, special locks, security personnel, or other authentication devices. Language in the template can be used for all facilities with Electronic Access controls.

For those facilities where electronic access control is not used, the measures used to manage physical access must be detailed here.

6 Physical Access Monitoring:

Detail the technical and procedural controls for monitoring physical access at all access points to the PSP, 24/7. Procedures for review of unauthorized access attempts must be included. Monitoring methods must be one of the following: alarm system or human observation of access points. If human observation is used it must include physical control by an authorized employee of access points. Language in the template can be used for all facilities with Electronic Access controls.

A sample access attempt report and inappropriate access attempt procedures can be found in Addendum B.

For those facilities where electronic access control is not used, the measures used to monitor physical access must be detailed here.

7 Logging Physical Access:

Detail methodology for logging all access to the PSP. This potentially includes employees and visitors, depending on the protection measures employed for the PSP. Logging shall record sufficient information to uniquely identify individuals and the time of access 24/7. Logging methods must be one of the following: computerized logging, video recording, or manual logging. Each PSP may have its own logging method. All logging methods must be documented in the PSP inventory (Addendum G). Language in the template can be used for all facilities.

8 Access Log Retention:

Detail the procedures for access log retention. Responsible position for actual log retention must be defined. This section must specify detailed information on where the logs will be kept and for how long. The length described in the template coordinates to the requirements in the standard. Language in the template can be used for all facilities.

9 Maintenance and Testing:

No text needed.

9.1 Physical Security System Maintenance:

This section details the local maintenance program used to ensure that all physical security systems function property. This includes maintenance of all physical components used to secure the PSP (locks, doors, windows, cameras, etc.). Language in the template can be used for all facilities with Electronic Access controls.

If there is no electronic Physical Access Control System used at a facility, local procedures for maintenance of all mechanical components must be developed. The maintenance procedures must be detailed here.

9.2 Physical Security System Testing:

This section details the local testing program used to ensure that all physical security systems function property. This includes testing of all physical components used to secure the PSP (locks, doors, windows, cameras, etc.). Language in the template can be used for all facilities with Electronic Access controls.

If there is no electronic Physical Access Control System used at a facility, local procedures for testing of all mechanical components must be developed. The testing procedures must be detailed here.

9.3 Outage Records:

This section details the requirements for retention of outage records regarding access controls, logging, and monitoring. All records must be kept for a minimum of 1 year.

Language in the template can be used for all facilities. If an electronic access control system is not used, the local responsible position must be incorporated.

A sample outage event log and procedures are located in Addendum F. See below for more information.

10 Approvals:

This section details the approval process for the plan. For consistency, the recommended level of final approval must at a minimum be at the area manager level. Additional approvals to ensure local coordination and implementation can be included. Language in the template includes several levels of approval and can be adopted for all facilities if specific positions are incorporated. Actual approval authorities must be defined on a local level.

Addendum A:

This section defines the procedures that are required to provide for secure access to PSP by employees and visitors who have not been previously issued specific PSP authorization. Language in the template can be used for all facilities. Any specific local procedures for visitor management must be incorporated to ensure seamless visitor management.

The visitor access log includes all required log details and can be easily reproduced for local use. Please note: the name/designation of the PSP must be included.

Addendum B:

This section defines the procedures that are required to report and manage the loss of a PSP access control card or key. Language in the template can be used for all facilities. Any specific local procedures for device loss must be incorporated to ensure seamless access management.

The access device loss report form includes all required loss details and can be easily reproduced for local use. Local responsible positions must be incorporated to ensure proper procedures are followed.

Addendum C:

This section defines the procedures that are required to manage and document the inappropriate use of Physical Access Controls. Language in the template can be used for all facilities. Additional refinement may be necessary to ensure the procedure addresses local actions and operating posture. For example, if a control center operator is going to make the determination regarding actions, those procedures need to be detailed here.

The access attempt report form includes all required details in the event of a possible intrusion and can easily be reproduced for local use. Local responsible positions and procedures must be incorporated to ensure proper procedures are followed.

The Investigating Officer referenced in Section 2 of the form must be a position locally designated to review any unauthorized access attempts. It may be the local security manager, but generally this will be someone else.

Addendum D:

This section defines the procedures that are required to manage the PSP access authorization process. Language in the template is designed for facilities with electronic access control systems, but can easily be modified to reflect a local manual process. Local responsible positions will need to be incorporated.

The access authorization request form includes all required information needed to document and track access and can easily be reproduced for local use. Language in the template can be used for all facilities, but local processes must be integrated. Local responsible positions will need to be incorporated.

Addendum E:

This section is to be used in conjunction with the Document History and the annual review and revision requirements. Information necessary includes: name of reviewer; title; date of review (completion); and reference information (if changes are made they need to be documented in the Document history and referenced here).

Addendum F:

This section defines the procedures that are required to manage the Physical Security and ECASS systems and document related maintenance, testing and outage activity. Language in the template can be used for all facilities with electronic access control systems. Local procedures must be integrated to ensure proper procedures are consistently followed. Local responsible positions will need to be incorporated.

If there is no electronic Physical Access Control System used at a facility, the following language must be inserted: No electronic physical access controls are employed in the protection of the PSP at XXX facility. This section is not applicable.

Addendum G:

This section contains the details of all PSP located within the facility and the physical protection measures used to secure them. If a single PSP is in place, the documentation will consist of only a few pages. If multiple PSP are utilized then a separate form must be completed for each.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

The instructions and inventory page contains the basic PSP information (number and title); together the number and title must correspond to the specific PSP identifier.

The detailed sheets will follow the inventory. Instructions for completion of the detailed sheets are contained on the sheets. All information regarding the specific CCA at the facility will be contained in this Addendum.

When completed, these sheets will provide the necessary details regarding each PSP to ensure compliance with the NERC requirements.