PG&E CIP-004 Access Management Procedure

SUMMARY

This document describes PG&E's electronic access procedure that, along with its partner Physical Access Procedure, satisfies the NERC CIP 004 access management R4 program requirements.

The scope of this procedure includes:

1. Authorized electronic access to:
    a. BES Cyber Systems Information (BCSI) Storage Repositories [R6.1]
    b. BES Cyber Systems [R4.1]
2. For the following cyber system classifications (aka "applicable cyber systems"):
    a. High Impact BES Cyber Systems (BCS) and Medium Impact BCS with External Routable Connectivity (ERC) and associated:
        i. Electronic Access Control or Monitoring Systems (EACMS)
        ii. Physical Access Control Systems (PACS)

This procedure includes the following inputs and outputs:

1. Inputs
    a. New system requests for registration into access permission systems
    b. BCSI repository or BCS system access requests
    c. Current permission records that require monthly and quarterly review and update cycles [R4.2 electronic access, R4.3]
2. Outputs
    a. New system registrations in access permission systems
    b. New BCS or BCSI permissions and access
    c. Updated permissions records

Level of Use: Informational Use

TARGET AUDIENCE

This procedure applies to all:

- Personnel who currently have or require access to applicable Cyber Systems.
- System Managers who facilitate access to Applicable Cyber Systems.
- System Owners for Applicable Cyber Systems.
- BCSI Repository Owners and BCSI Custodians.
- Supervisors and their authorized delegates whose direct reports have or require access to Applicable Cyber Systems.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

- Identity and Access Management (IAM) Compliance personnel.
- Personnel with a Security or Compliance role at PG&E.

SAFETY

Tasks and requirements described in this procedure do not raise the risk of a specific hazard to personnel, the public, or equipment.

BEFORE YOU START

READ:

- Utility Standard: TD-1204S, "PG&E CIP-004: Cyber Security Personnel and Training"
- Utility Standard: SEC-3006S, "Identity and Access Management Standard"

COMPLETE:

1. PRA background check
    a. Current PRA required for past 7 years (unless minor status was less than 7 years ago).
2. Cyber Security Training
    a. CORP-0804

TABLE OF CONTENTS

SUBSECTION	TITLE	PAGE
2	System Integration	4
3	Authorization Processes (R4.1)	4
4	Quarterly Authorization Review Processes (R4.2, R6.2)	5
5	PAAR Annual Access Certification Processes for BES Systems (R4.3)	7
6	Non-PAAR Access Model Certification for BES Systems (R4.3)	8

WARNING

Employees found to have violated these requirements may be subject to disciplinary action, up to and including termination of employment.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

PROCEDURE STEPS

1 Access Model Development

1.1 System Owner/Manager(s) or BCSI Owner/Custodian(s)

1. GET the CIP-004 Access Model Template from the TO-CIP-004 Work Site.
2. FILL OUT the template PER instructions on the first tab, including:
   a. System, repository, or asset information
   b. List of all users, built-in, default, system or shared accounts
   c. List of all provisioned groups
   d. Permission levels for all groups and accounts
   e. Any other requested data in the template.
3. STORE CIP-004 Access Model Template.
   a. USE this SharePoint Location:
      (1) System and Repository Access Models
   b. USE this naming convention:
      (1) [APP-ID/Repository Name] – Access Model – Draft.xlsx", in a folder named for your system/repository.
      (2) FILL IN above bracketed APP-ID section only ("Access Model – Draft.xlsx" is same for every template name).

NOTE

1. IF all access is integrated in MEA OR PAPM, THEN the system or repository is considered "Enterprise Managed" for any process referencing associated security applications.
2. IF access is not integrated to MEA OR PAPM, THEN the system or repository is considered "System Owner" Managed for any process referencing associated security applications.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

2 System Integration

2.1 Where technically feasible, INTEGRATE Applicable Cyber System into PG&E's MyElectronicAccess (MEA) AND, if required, Privileged Access & Password Management (PAPM).

1. SUBMIT request PER MyElectronicAccess (MEA) Onboarding.
2. For High Impact BES Cyber Assets OR EACMS SUBMIT request PER CyberSecurity Services (pge.com).
    a. High Impact BCA or EACMS shared accounts require an MEA disconnected entitlement if not integrated into PAPM.
3. IF not technically feasible to register template information with PAPM, THEN:
    a. SUBMIT Exception PER EP-IT Potential Non-Conformance.
    b. REQUEST MEA system access through disconnected entitlements.
        (1) SUBMIT request PER MyElectronicAccess (MEA) Onboarding.
    c. UPDATE CIP-004 Access Model Template with additional notes PER template first tab instructions for all relevant information:
4. STORE CIP-004 Access Model Template.
    a. USE this SharePoint Location:
        (1) System and Repository Access Models
5. The access model should be maintained by the System or BCSI Repository Owner moving forward when changes occur.

3 Authorization Processes (R4.1)

3.1 User

1. REQUEST My Electronic Access (MEA) permissions PER MEA User Guide.

3.2 Supervisor or Role Owner (or authorized approver)

1. APPROVE OR REJECT permission request PER MEA User Guide.

3.3 System Owner/Manager(s) or BCSI Owner/Custodian(s)

1. IF there are Disconnected Entitlements, THEN,

©2025 Pacific Gas and Electric Company. All rights reserved.

a. MEA will CREATE service request for Owner, Manager, or Custodian to manually provision system access.

2. PROVISION the access to the appropriate asset or repository.

3. UPDATE the Access Model with new access information.

4. STORE the Access Model in your repository.

a. USE this SharePoint Location:

(1) System and Repository Access Models

4 Quarterly Authorization Review Processes (R4.2, R6.2)

NOTE

PG&E's quarterly authorization review process includes both BES systems for CIP-004-7 R4.2 and BCSI Repositories for R6.2. An additional annual review of BCSI Repositories is not required by CIP-004-7, however PG&E performs this annual review. (see section 5)

4.1 IAM Operations CONDUCTS quarterly reviews to ensure entitlements are configured appropriately for authorization and certification.

1. RETREIVE entitlements report from MEA: MEA NERC Catalog Report.

a. ANALYZE report to ensure entitlements for the Applicable Cyber Systems are configured for:

(1) Access Review Required

(2) Supervisor and Role Owner Approval

(3) Quarterly Certification Cycle

(4) PRA prerequisite required

(5) CORP-0804 prerequisite required

2. IF misconfigurations are identified, THEN:

a. REVIEW issue details.

b. DETERMINE cause of the issue and remedial actions required.

c. TRACK remediation activities assigned to stakeholders until resolved.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

(1) BES/BCSI Quarterly Authorization R4.2/6.2 - Remediation

d. DOCUMENT cause of the issue and any required remediation.

3. IF no misconfigurations are identified, THEN:

   a. PROCEED to next step.

4. STORE documentation in appropriate review quarter within the BES/BCSI Quarterly Authorization R4.2/6.2 folder.

5. IF it is not time for a Quarterly Review, THEN,

   a. END Procedure.

6. IF it is time for a Quarterly Review, THEN:

   a. VERIFY the three-monthly reports stored in the CIP-004 Working Site > R4.2 > Enterprise Managed Evidence folder are accurate and complete.

   b. UPLOAD the evidence to Appian.

   c. END Procedure.

NOTE

Supervisors and Role Owners reauthorize electronic access for Enterprise Managed or System Owner Managed systems PER MEA User Guide.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

5 PAAR Annual Access Certification Processes for BES Systems (R4.3)

NOTE

PG&E performs separate annual certifications for both BES systems (CIP-004-7 R4.3) and BCSI Repositories. The BCSI Repositories annual review is not required by CIP-004-7, however PG&E performs this review for additional security.

5.1 IAM Compliance:

1. PAAR Access Certification Campaign Initiation for BES System

   a. On an annual basis the IAM NERC-CIP 004 Compliance Administrator will initiate the annual certification campaign using PAAR starting May - July.

   b. Once a Certification Campaign is started, each BES System Owner will receive a PAAR generated email notification informing them of the start and end dates of the campaign.

2. PAAR Access Certification Campaign Initiation for BCSI Repositories

   a. On an annual basis the IAM NERC-CIP 004 Compliance Administrator will initiate the annual certification campaign using PAAR starting July - September.

   b. Once a Certification Campaign is started, each BCSI Repository Owner (RO) will receive a PAAR generated email notification informing them of the start and end dates of the campaign.

5.2 System Owner / Repository Owner:

a. Once the Compliance Admin starts the campaign, the System Owner (SO) or Repository Owner (RO) handles processing the items assigned to their certification queue.

b. RO/SO access PAAR certification queue and reviews entitlements/member groups associated with their Repository to confirm their validity. ENSURE information is accurate and required for business operations:

   (1) Groups and Entitlements

   (2) Accounts

   (3) Privilege level

   (4) General Information (Asset information, application data, system ratings, etc.)

c. UPDATE PAAR with appropriate comments, if updates/changes to account is required.

©2025 Pacific Gas and Electric Company. All rights reserved.

6 Non-PAAR Access Model Certification for BES Systems (R4.3)

NOTE

If a BES System or BCSI Repository cannot integrate with PAAR, a non-integrated "manual" certification must be performed.

1. System Owners/BCSI Custodians:
   a. RECEIVE annual notice from IAM Operations to initiate certification.
   b. REVIEW current CIP-004 Access Model Template located in system folder:
      (1) System and Repository Access Models
   c. ENSURE information is accurate and required for business operations:
   d. Groups and Entitlements
   e. Accounts
   f. Privilege level
   g. General Information (Asset information, application data, system ratings, etc.)
2. UPDATE CIP-004 Access Model Template with appropriate changes to its Change Log.
   a. INCLUDE certification completion details and date in change log.
3. STORE CIP-004 Access Model Template in system folder:
   a. System and Repository Access Models
4. IAM Operations:
   a. RETRIEVE latest CIP-004 Access Model Template from system folder.
      (1) System and Repository Access Models
   b. CONFIRM all access is certified for last 12 months.
   c. UPLOAD evidence to Evidence Repository.
   d. IF any access has not been certified, THEN,
      (1) THEN ENGAGE NERC CIP Compliance to begin self-report processes per CAP Procedure.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

e. OTHERWISE END procedure.

END of Instructions

DEFINITIONS

Applicable Cyber Systems: BCS and associated EACMS and PACS identified within the CIP-002 inventory and authorized storage locations for BES Cyber System Information (BCSI) identified within CIP-011 inventory that are within scope of NERC CIP-004-7 R4 requirements.

BES Cyber System (BCS): One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information (BCSI): Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Bulk Electric System (BES): Predominantly all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.

Connected Entitlement: A connected entitlement is an MEA entitlement which provides for the authorization of access and controls the provisioning of access on the applicable cyber system.

Disconnected Entitlement: A disconnected entitlement is an MEA entitlement which provides for the authorization of access but control of the provisioning of access on the applicable cyber system is managed by the System Owner or System Manager(s).

Electronic Access Control or Monitoring Systems (EACMS): Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

Enterprise Managed Access: Access which is authorized, controlled, and managed by enterprise systems and automated processes versus local management by the System Owner.

External Routable Connectivity (ERC): The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

MyElectronicAccess (MEA): A suite of identity management solutions that perform identity lifecycle management functions and assist PG&E in complying with NERC CIP requirements.

MyPhysicalAccess (MPA): is the self-service portal for requesting physical access to PG&E locations; e.g. substations, offices, yards, etc. This web application interfaces with Quantum SAFE, the physical access control system, and provides the authorization of unescorted physical access, quarterly access reviews, and revocation of access when needed.

Personnel Risk Assessment (PRA): Background check performed typically as a condition of hire that must be completed prior to receiving permission for access to BES Cyber Systems.

Physical Access Control Systems (PACS): Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Privileged Access Automated Reporting (PAAR) application that automatically connects to NERC BES Cyber Systems, EACMS, PACS and BCSI target systems to collect account information.

Privileged Account Password Management (PAPM): Internal security tool(s) that protect and control passwords to reduce risk by identifying, securely storing, and centrally managing every credential that provides elevated access.

System Access Model: A system access model is a baseline of the provisioned accounts, groups, roles, and associated permissions for a system as it is applied to the various assets, applications, databases, and other areas of provisioned electronic access.

System Manager: System Manager(s) (also referred to as Delegates or System SMEs) manage, operate and maintain servers, network appliances, workstations, and related applications to help ensure the efficient operation and enhance the reliability of the BES. This includes system, database, and application administrators or any other delegate who manages the BCS.

System Owner: System Owners are the accountable owners of a BES Cyber System. They typically are the final authority on decisions made for the operation, management, and sustainment of the system.

System Owner Managed Access: Access which is authorized by enterprise systems but controlled and managed at the local system level by the System Owner or System Manager(s). System Owner Managed Access applies to areas of access that are not integrated with one or more of the systems identified (e.g. if the application has locally managed access due to exceptional circumstance and the system is integrated with MEA and ADAM, the System Owner would only apply the process(es) to the application access, when identified).

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

IMPLEMENTATION RESPONSIBILITIES

IAM Operations is responsible for 1) managing the daily operations of MEA, -PAAR, and other tools that support internal controls and 2) maintaining the compliance program.
System Owners, System Managers, and End Users are responsible for following the prescribed processes in full and complying with defined requirements.

GOVERNING DOCUMENT

- Utility Standard: TD-1204S, “Cyber Security Personnel and Training”
- Utility Standard: TD-1202S, “BES Cyber Systems Identification and Classification”
- Utility Standard: 1211S, “Cyber Security- Information Protection Standard”
- Utility Standard: SEC-3006S, “Identity and Access Management Standard”

COMPLIANCE REQUIREMENT / REGULATORY COMMITMENT

Records and Information Management:
Information or records generated by this procedure must be managed in accordance with the Enterprise Records and Information (ERIM) program Policy, Standards and Enterprise Records Retention Schedule (ERRS). REFER GOV-7101S, “Enterprise Records and Information Management Standard” and related standards. Management of records includes, but is not limited to:

- Integrity
- Storage
- Retention and Disposition
- Classification and Protection

NERC CIP Compliance

CIP-004: Cyber Security – Personnel & Training

REFERENCE DOCUMENTS

Developmental References:

- MyElectronicAccess – Technical Standard
- Utility Procedure TD-1204P-02, “PG&E CIP-004 Cyber Security Training Program”
- Utility Procedure TD-1204P-03, “Personnel Risk Assessment (PRA) for PG&E Employees”
- Utility Procedure TD-1204P-06, “Personnel Risk Assessment (PRA) for Non-Employee Workers
- Utility Procedure: TD-1210P-03, “PG&E CIP-010: Cyber Security – Vulnerability Assessment”
- RISK-4050P-01, "NERC Investigation, Self-Report and Mitigation Procedure"
- SEC-1100P-01 EP-IT GRC Potential Non-Conformance or Compliance Procedure

Supplemental References:

- Utility Procedure TD-1204P-04, “PG&E CIP-004 Physical Access Management Program”

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

- Utility Procedure TD-1204P-7, "PG&E CIP-004 Cyber Security – Logical Access Management"
- System and Repository Access Models
- CIP-004 Access Model Template
- TO-CIP-004 Work Site
- MyElectronicAccess (MEA) Onboarding
- CyberSecurity Services (pge.com)
- MEA NERC Catalog Report
- IAM Compliance - Remediation Tracking
- CIP-004-7 Working Site > R4.2 > Enterprise Managed Evidence
- Evidence Repository (Appian – Permissions Required)
- MEA User Guide

APPENDICES

N/A

ATTACHMENTS

1. MEA User Guide

DOCUMENT RECISION

N/A

DOCUMENT APPROVER

[redacted]), IAM Operations Senior Manager, Cybersecurity

DOCUMENT OWNER

[redacted]), Director, Cybersecurity

DOCUMENT CONTACT

[redacted]), IT Solutions Engineer, Expert

REVISION NOTES

Rev	When	Where	What Changed?
5	07/18/2023	Global	Revised entire document to align with new compliance direction and process changes.
6	10/31/2023	Global	Updates for CIP-004-7 and ownership changes.
7	12/4/2024	Sections 4, 5, 6	Section 4: updated due to CIP-004-7 requirement change from R4.4 to R6.2 Section 5: Added section 5 for annual review of BES

©2025 Pacific Gas and Electric Company. All rights reserved.

PG&E CIP-004 Access Management Procedure

			System and BCSI Repositories using PAAR Section 6: Added new section for non-PAAR reviews.

©2025 Pacific Gas and Electric Company. All rights reserved.