

Introduction

The reliability of the energy grid depends not only on physical assets, but cyber assets. The North American Electric Reliability Corporation (NERC) realized that, along with protecting the physical assets, Critical Cyber Assets also need to be protected to keep the energy grid secure.

Physical Assets

Control centers, substations, plants, etc.

Cyber Assets

Computer hardware, software, communication networks – anything that can control the flow of power through the energy grid.

To help protect the Critical Cyber Assets, NERC created nine mandatory Critical Infrastructure Protection Standards (CIPS) for all energy companies.

If PacifiCorp does not comply with these standards, the results could include fines. It could also open us up to possible malicious activity on our critical assets.

CIP-001 Sabotage Reporting

PacifiCorp must provide Emergency and Trouble Notification guidelines to its Grid Operators and staff. **If you are involved with Grid operation, you need to be familiar with this document!**

This document covers:

- Under what circumstances you are required to report a disturbance (e.g., key equipment failure, system-wide reductions in voltage, act of vandalism).
- To whom you report the disturbance, how quickly you must respond and what forms need to be filled out.

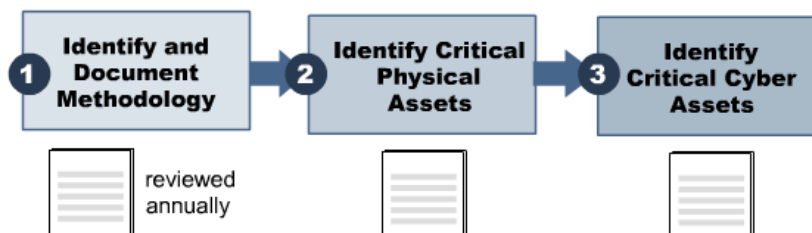
Surveillance usually occurs before any sabotage. Be aware of suspicious individuals and activity and report it to the Enterprise Help Desk immediately (x5555).

Emergency & Trouble
Notification Guidelines



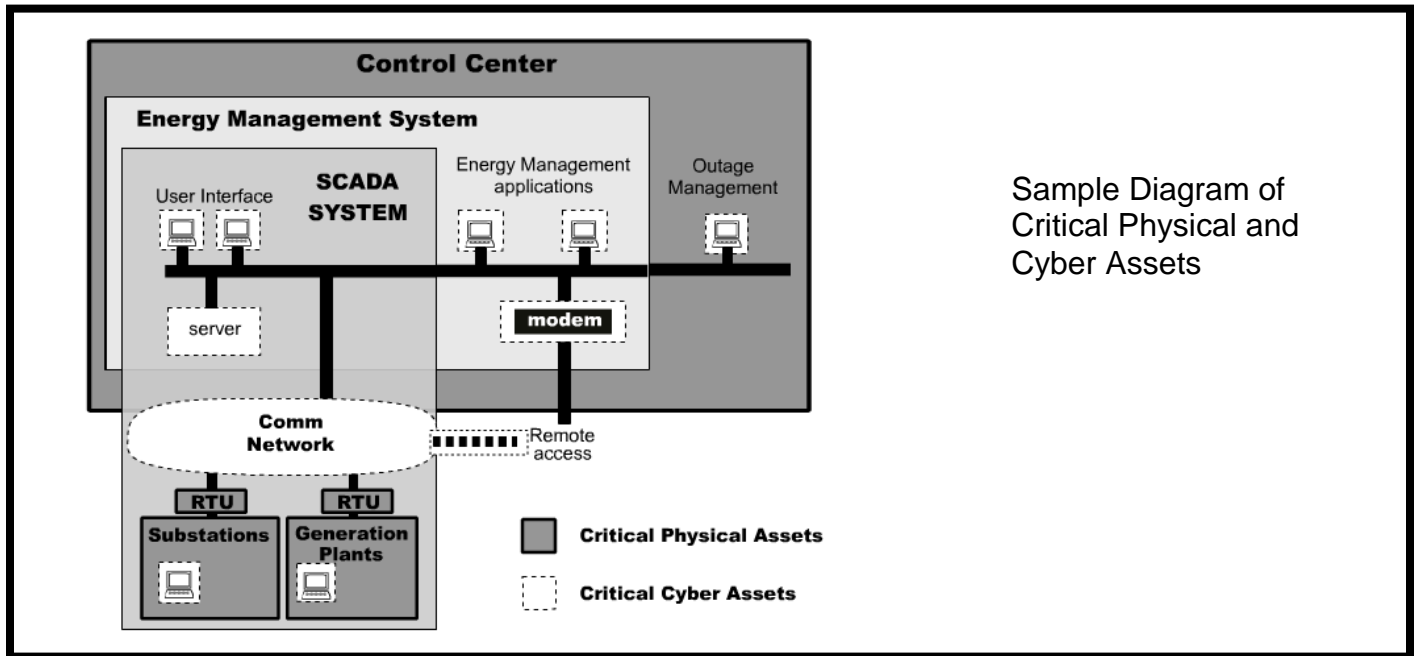
CIP-002 Critical Cyber Asset Identification

The first step in protecting Critical Cyber Assets is identifying them. CIP-002 focuses on this identification process.



PacifiCorp must:

- Identify and document a methodology to identify Critical Assets.
- Develop a list of Critical Physical Assets based on the above methodology (e.g., key substations, most generation plants, critical control centers).
- Develop a list of Critical Cyber Assets essential to the operation of the Critical Physical Assets. The list includes computer systems and communication networks that support and control the critical physical assets (e.g., RANGER/EMS, Network Infrastructure (non-EMS), Microwave, DAXs, Fiber Nodes, Channel Banks and DCS).



Sample Diagram of Critical Physical and Cyber Assets

CIP-003 Security Management Controls (create Cyber Security Plan)

Now that the Critical Cyber Assets are identified, PacifiCorp needs to figure out how to protect them. PacifiCorp must:

- Implement and document a cyber security policy on how to secure Critical Cyber Assets. Policy must be detailed and accurate, reviewed annually, and available to all personnel who deal with Critical Cyber Assets.
- Detail document exceptions: any instances where compliance to the policy is not possible must be promptly documented and approved.
- Assign senior manager for CIP compliance (Pat Reiten is the PacifiCorp Senior Manager).
- Protect and classify Information. Examples: floor plans of computer centers, disaster recovery plans, security configuration, critical network connectivity diagrams.
- Create and maintain list of access privileges. List should include people who are authorized to grant both physical and electronic access to protected information and those who have been granted access. List must be reviewed annually.
- Create and document Change Management process: establish and document process for adding, modifying, replacing or removing any Critical Cyber Asset hardware and software.

CIP-004 Personnel and Training

Now that the Critical Cyber Assets have been identified and a plan to protect them created, PacifiCorp needs to create a program to train the appropriate people on the Cyber Security Plan. As part of this, PacifiCorp must:

- Create and document a security awareness program for people having unescorted access to Critical Cyber Assets via quarterly presentations, web-based training, emails, intranet articles.
- Implement an annual cyber security training program for all personnel, including contractors and vendors, prior to giving them unescorted access to Critical Cyber Assets.
- Training content must include: proper use of Critical Cyber Assets, physical and electronic access controls, action plans for responding to a cyber security incident. Training records must be kept and available for audit.
- Conduct personnel risk assessment, i.e., background checks, social security number verification, seven-year criminal check, review of assessment every seven years.
- Maintain a list of employees with unescorted access to Critical Cyber Assets (including the type and level of access they have). List should be updated within 7 calendar days of any changes. Access to Critical Cyber Assets should be revoked within 24 hours for personnel terminated for cause. For personnel who no longer need access to CCA, their access should be removed within 7 calendar days.

CIP-005 Electronic Security Perimeters

In CIP-002, we identified Critical Cyber Assets. The first step in protecting them is to create “electronic security perimeters.” Electronic security perimeters monitor and control access to the Critical Cyber Assets.



PacifiCorp must:

- Create electronic security perimeters. Every critical cyber asset must reside within an electronic perimeter and all points to the perimeter must be identified and documented.
- Protect access points to the electronic security perimeter, once identified must create and document procedures for controlling access points (e.g., dial-up access, authenticating anyone asking for external access, enabling only ports and services required for key operations).
- Set up 24/7 monitoring of activity at access points, set up alerts to notify designated personnel of unauthorized access, set up monitoring processes for dial-up accessible Critical Cyber Assets. If it is not feasible to have 24/7 monitoring, must have logs of access attempts and review them at least every 90 days.
- Perform annual vulnerability assessment of all access points – review of enabled access points, review of controls for all default accounts and passwords. After documenting review, include plan to correct vulnerabilities.
- Review, update and maintain all documentation. Review must be done annually, any changes must be reflected in documentation within 90 days, electronic access logs must be kept for at least 90 days.

CIP-006 Physical Security of Critical Cyber Assets

CIP-005 focused on electronic perimeters to protect Critical Cyber Assets. CIP-006 focuses on physical security measures to protect these assets. PacifiCorp must:

- Create and maintain a physical security plan. Examples: process to monitor physical access to the perimeter, procedures for managing visitors passes, escorting visitors or nonauthorized personnel, handling access requests and revoking someone’s access. Plan must be updated within 30 days of any physical security system changes.
- Implement physical access controls to manage access 24/7. Suggested methods: security card keys, special locks, security personnel.
- Monitor access at all physical access points.
- Log physical access attempts by using at least one of the following methods: computerized logging or manual logging.
- PacifiCorp must retain access logs for 90 days.
- Maintain and test physical security systems (all mechanisms must be tested at least every three years, must retain exception records for at least one year).



CIP-007 Systems Security Management

Once you have system controls in place to protect the electronic security perimeter, the next step is to protect and maintain these system controls. PacifiCorp must:

- Test procedures (make sure any changes to the cyber assets within the electronic security perimeter do not alter the effectiveness of the controls in place. Examples: version upgrades of software, software security patches, service packs). Must document all test results.
- Enable only necessary ports and services.
- Manage security patches. Must establish program to test, track and install applicable cyber security software patches for all cyber assets within the electronic security perimeters.
- Protect systems from malicious software (use anti-virus software prevention tools and then establish process to keep anti-virus software updated).
- Manage and verify all user activity.
- Monitor cyber security system events. PacifiCorp must review and retain all logs of any abnormal system events.
- Dispose of cyber assets properly. Set up effective procedures for disposal or reuse of any cyber assets that were within the electronic security perimeter. Prior to disposal or redeployment of such assets, must erase any sensitive data and retain documentation that this was done.
- Perform cyber vulnerability assessment.
- Review and update CIP-007 documentation annually and document system changes/updates within 30 days.



CIP-008 Incident Reporting and Response Planning

If a cyber security incident happens, PacifiCorp needs to be prepared to respond to it. PacifiCorp must:

- Implement a cyber security incident response plan. Plan how to classify events as reportable cyber security incidents, assign roles/responsibilities in case of an incident, and plan procedures for testing.
- Maintain cyber security incident documentation (must keep relevant documentation related to cyber security incidents for 3 calendar years).

CIP-009 Recovery Plans for Critical Cyber Assets

After a cyber security incident, PacifiCorp may need to recover. To prepare for this, PacifiCorp must:

- Develop and maintain a recovery plan for Critical Cyber Assets
- Exercise the recovery plan annually.
- Update the recovery plan based on testing (updates must be communicated within 30 days of change).
- Backup and restore.
- Test backup media annually.
- Understand your responsibilities



Compliance

Implementation of the standards is a gradual process. NERC has established four increasing levels of compliance and has established implementation dates for each of the requirements of the CIP Standards. Full compliance with all requirements for all CIP standards is currently set to January 1, 2011.



Summary

CIP Standard	Summary
CIP -001	How and when to respond to Sabotage incidents
Identification and protection of Critical Cyber Assets	
CIP-002	First step in protecting Critical Cyber Assets it to identify them.
CIP-003	Now that they are identified, you need to create a Cyber Security Plan on how to protect them.
CIP-004	You've got the Cyber Security Plan now, but now need to identify who needs to be trained on it and then train them.
CIP-005	Now, you need to begin implementing the Cyber Security Plan. Start by protecting Critical Cyber Assets by creating an Electronic Security Perimeter around them.
CIP-006	Further protect Critical Cyber Assets by creating a Physical Security Perimeter around them
CIP-007	Now that you have created Electronic and Physical Security Perimeters, you need to protect and maintain them. You also need to monitor them for incidents.
CIP-008	If a cyber security incident does occur, you need to have a plan for how to respond.
CIP-009	You need to know how to recover from any impact from a cyber security incident.