

# Bonneville Power Administration

## NERC CIP PHYSICAL SECURITY IMPLEMENTATION

Security & Emergency Response



# Outline

1. Purpose
2. BPA Facts
3. Brief NERC CIP Overview
4. NERC CIP Standards
5. NERC CIP -- Physical Security
6. Challenges
7. Questions



# Purpose

Provide a brief overview of how the BPA Security Office interpreted NERC CIP Standards relating to Protecting BPA's Assets, how they implemented security upgrades to meet the standards, and some of the challenges faced.



3/22/2010

Slide 3

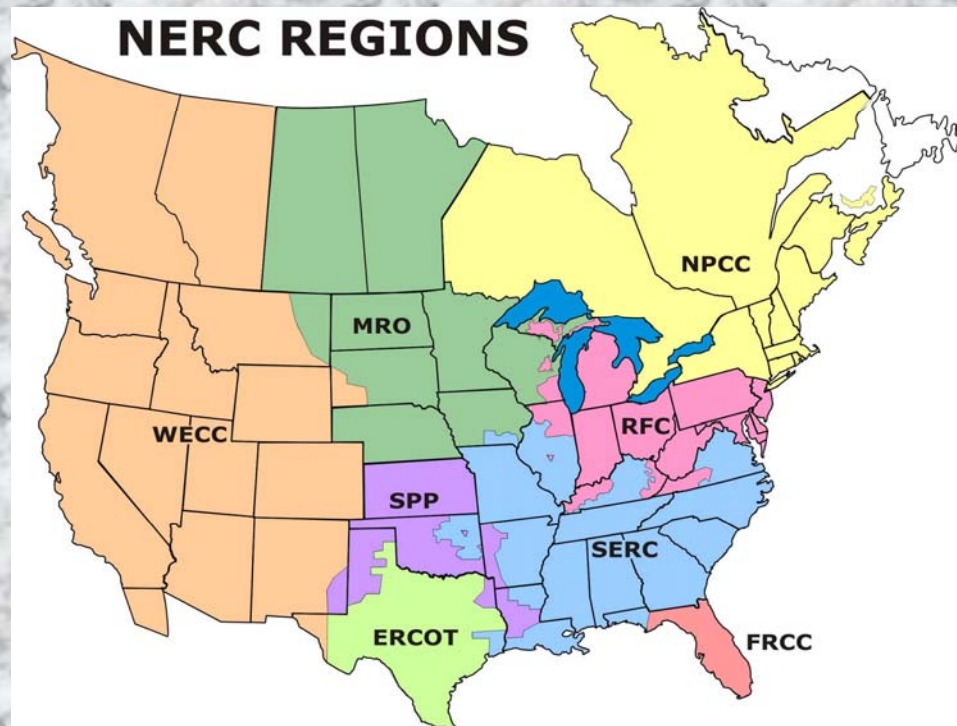


# BPA Facts 2008

- **BPA Established:** 1937
- **Service Area (square miles):** 300,000
  - Oregon, Washington, Idaho
  - California, Idaho, Utah, Wyoming
- **Transmission Line (circuit miles):** 15,238
- **BPA Substations:** 259
- **Hydro Projects (Federal—Non BPA):** 31 dams



# NERC - North American Electric Reliability Corporation



3/22/2010

- A voluntary organization in operation since 1968.
- NERC's mission is to make bulk electricity reliable, adequate, and secure.
- NERC is made up of eight regions that oversee the reliability and operation of the Bulk Electric System.
- Entities may have assets in multiple regions.
- Entities may have registered as performing multiple functions in one or more regions.

# What is CIP?

## CIP - Critical Infrastructure Protection

- A set of standards created to reduce risks to the reliability of the "Bulk Electric Systems" from any compromise of Critical Cyber Assets.
- Standards CIP 002 through CIP 009



# NERC CIP Categorization

- The NERC CIP mandates are broken down into nine standards, eight of which (CIP 002 through CIP 009 comprising 41 different requirements) have been specified for implementation within BPA.
- The requirements establish organization roles and responsibilities, policies, guidelines, and procedures.
- To achieve compliance, the NERC-CIP standards must be incorporated into BPA activities and management decision-making processes.
- Full compliance is defined as meeting the letter and intent of each NERC-CIP requirement.



# NERC CIP Standards

CIP002: Critical Cyber Asset Identification

**CIP003: Security Management Controls**

**CIP004: Personnel and Training**

CIP005: Electronic Security Perimeter(s)

**CIP006: Physical Security**

CIP007: Systems Security Management

CIP008: Incident Reporting and Response Planning

CIP009: Recovery Plans for Critical Cyber Assets

Total of 41 Requirements (Control Center & Field = 82)



# CIP – 002 Critical Cyber Assets

- R1 Critical Asset Identification Method
- R2 Critical Asset Identification
- R3 Critical Cyber Asset Identification
- R4 Annual Approval

**Critical Asset:** Facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

**Cyber Asset:** Programmable electronic devices and communications networks including hardware, software and data.

**Critical Cyber Asset:** Cyber Assets essential to the reliable operation of Critical Assets.



# CIP – 003 Security Management Controls

---

- R1 Cyber Security Policy
- R2 Leadership
- R3 Exceptions
- **R4 Information Protection**
- R5 Access Control
- R6 Change Control and Configuration Management



# Information Protection

- BPA's Official Use Only (OUO) program was updated to provides clarified guidance and policy. NERC CIP information was added to the Critical Program Information List (CPIL).
- The Transmission Information System Security Manager developed policy and guidance that flows from BPA's OUO program.

The policies, processes, and procedures must be reviewed annually.



# CIP – 004 Personnel and Training

- R1 Awareness
- R2 Training
- R3 Personnel Risk Assessments (PRA)
- R4 Access



# Personnel Risk Assessments (PRA)

- All personnel having unescorted access to Critical Cyber Assets are required to undergo a 7 year recurring risk assessment and Personal Identity Verification (PIV).
- BPA has approximately 2,000 employees requiring unescorted access.
- BPA uses the Office of Personnel Management (OPM) for processing the criminal history checks.
- Homeland Security Presidential Directive – 12 (HSPD-12): Requires a background check for unescorted access to government facilities.



# CIP – 006 Physical Security

- R1 Physical Security Plan (9 Sub Requirements)
- R2 Physical Access Controls
- R3 Monitoring Physical Access
- R4 Logging Physical Access
- R5 Access Log Retention
- R6 Maintenance and Testing



# Physical Security

- **Scope:**
  - **Over 60 Facilities** which includes Control Centers, Power Scheduling Centers, facilities housing access control servers, and Critical Field Assets
  - Facility upgrades, training, policy/process/procedure development
- **Efficiencies:**
  - **Homeland Security Presidential 12**
  - **DOE's new Graded Security Plan**

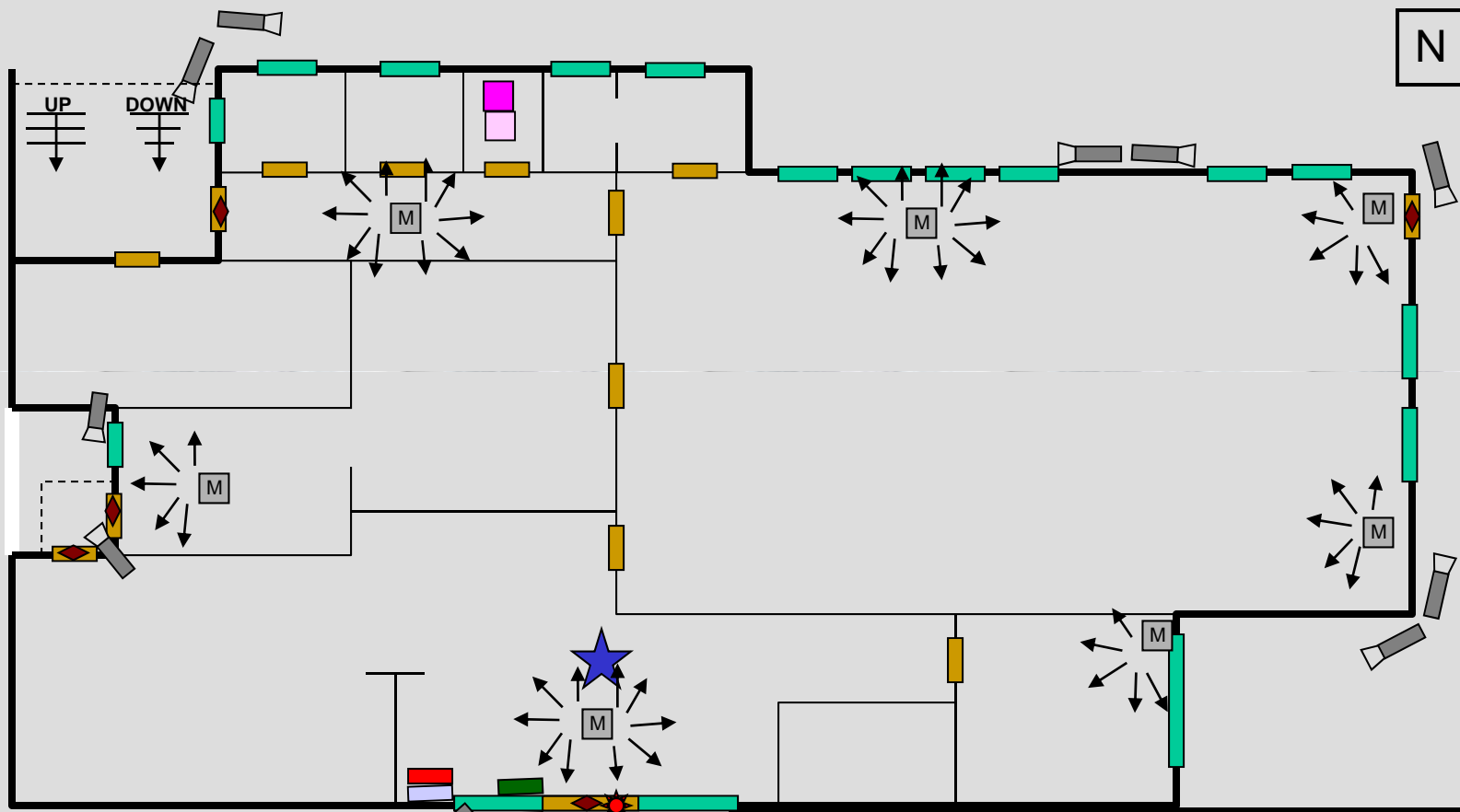
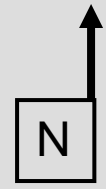


# Physical Security

- Physical Security Plan (Each Site will have a site specific plan)
  - Diagrams
  - Policy, processes, procedures
  - Reviewed at least annually, or within 30 days of a change
- Access Controls: Card Key & PIN (authorized personnel only)
- Monitoring Access Points: Alarm System
- Logging Access: Card Key
- Log Retention: Prowatch Database
- Maintenance and Testing: Annually



### Physical Security Perimeter (Control House)



Main Control House Door

PTZ

LEGEND	
	Camera
	Alarm Contact
	Entry Reader w/Pin Pad
	Exit Reader
	Alarm shutoff
	Siren
	Exit Buzzer
	Motion Detection
	DVR
	Window
	Alarm Control Panel
	Door
	Keypad Display

# Challenges

- Limited time to develop, document, and implement each NERC CIP requirement.
  - Aggressive schedules for all projects
  - Leverage previous work and between CCs and Field
- CIP requirements span multiple organizations within BPA
- BPA's audit is scheduled for November 2010.
  - All 8 standards and 41 requirements (Control Centers Only)
  - Significant sanctions and heavy fines are VERY possible if BPA does not pass audits



# Challenges

- Meeting Compliance Deadlines
- Adequate resources (near term versus long term)
  - All standards and requirements require ongoing maintenance, do we have the resources to maintain what we have put in place?
- Conflicting priorities
  - NERC CIP versus DOE GSP & other DOE Requirements
  - NERC CIP versus FISMA
- NERC is drafting the next set of standards
- Proposed legislation: Protection of Transformers



# Sanctions Penalty Matrix

		Violation Severity Level							
		Lower		Moderate		High		Severe	
		Range Limits		Range Limits		Range Limits		Range Limits	
Violation Risk Factor	Low	High	Low	High	Low	High	Low	High	
	Lower	\$1,000	\$3,000	\$2,000	\$7,500	\$3,000	\$15,000	\$5,000	\$25,000
Medium	\$2,000	\$30,000	\$4,000	\$100,000	\$6,000	\$200,000	\$10,000	\$335,000	
High	\$4,000	\$125,000	\$8,000	\$300,000	\$12,000	\$625,000	\$20,000	\$1,000,000	

\* Violations are incurred on a per day basis



# Questions

## Contact Information

**Erik Smith**  
**NERC CIP Program Manager**  
**Security and Emergency Response**  
**Bonneville Power Administration**

**[easmith@bpa.gov](mailto:easmith@bpa.gov)**

**503 230-5278**

