



CIP-005

**Access Control,
Monitoring and Logging**

**EI Spring Security
Committee Meeting
Cyber Security Breakout**

**March 21st 2007
Long Beach, CA**

Patrick Miller, CISA CISSP-ISSAP



PacifiCorp Stats

- Owned by MidAmerican Energy Holdings Company
- Made up of three separate organizations
 - PacifiCorp Energy, Pacific Power and Rocky Mountain Power
- Headquarters in Portland, OR
- ~6650 Employees
- ~136,000 square miles of service area over six states
 - Oregon, Washington, California, Utah, Wyoming, Idaho
- ~1.6 million customers
- ~8,200 MW of generation

Define the Perimeter

- Challenges identifying *everything* – both critical and non-critical
- What qualifies as a perimeter?
 - DMZ, VLAN, VPN (client and site-to-site)
 - Don't forget about defense-in-depth
- Firewall questions...
 - Which one? Is heterogeneity a good thing?
 - For a DMZ, which interface is the *real* perimeter?
 - Management and administration from outside the perimeter?
- One big [interconnected] perimeter vs. several small perimeters

Access Controls

- Remote access vs. operational access
- Multi-factor authentication challenges
- Citrix, SSL-VPN and other ways to get through
- Different credentials for different zones
- Network Access Control (NAC) and similar models
- Dial-up controls and challenges
 - P3-challenger hardware encryption
 - Modem banks
 - Processes for circuit procurement and inventory

Monitoring Access

- NIDS vs. HIDS
- Have you heard about NetIntercept?
- Security Event Monitoring = Bigfoot (do they really exist?)
 - Pick one: Loch Ness, space aliens, Kaiser Sose, El Chupacabre, the Coelacanth, etc...
 - How many products/vendors were tried (and failed)
 - No vendor has hit the mark yet for an organization of our size
- The Security Intelligence System (SIS)
 - Much is already available in open-source offerings, just add glue
 - Hardware is cheap: 10TB+
 - Bandwidth is no issue
 - Customization is powerful
 - Data can be used for *many* purposes
- Manual log review is very time consuming and often inconsistent

Vulnerability Assessment

- Many vendors offer services, but choose wisely
 - Not all vendors have the necessary skill set, even if they say they do
 - If you are willing, sign a CRADA with INL – well worth it
 - Third parties usually bring about the greatest degree of change
- Can be performed by in-house staff with appropriate skills
 - Manual review is best, but also most time consuming
 - Be *very, very* careful with vulnerability scanners; plan for problems
 - War-dialers are great -- if you know all your numbers
 - Use direct POTS lines instead of PBX
 - Don't forget about encryption keys

Questions?

Patrick C. Miller

CISA, CISSP-ISSAP, SSCP, NSA-IAM, TCP, SCP

Sr. Information Security Consultant

patrick.miller@pacificorp.com

503.813.7014