Changes since video was filmed...

- Slide 7 - Document Access Control Mechanisms: The requirement to display acceptable use banners has been retired per the Paragraph 81 project

December 2013
CIP-005: Electronic Security Perimeter

Kevin B. Perry
kperry.re@spp.org · 501.614.3251
The Expectations

• Critical Cyber Asset identification drives the process, not the other way around.

• The steps are:
  1. Identify the Critical Cyber Assets
  2. Draw the Electronic Security Perimeter (ESP)
  3. Identify everything else within the ESP
  4. Identify the ESP Access Points
  5. Document... Document... Document!
Critical Cyber Asset Identification

- Completed by performing CIP-002-3, Requirement R3
- Pay attention to:
  - Cyber Asset and Critical Cyber Asset definitions in the NERC Glossary
  - The three qualifying criteria found in CIP-002-3, Requirement R3:
    1. Use of a routable protocol to communicate outside of the ESP – really means outside of the facility (asset) since the ESP has not been defined yet
    2. Use of a routable protocol within a control center
    3. Dial-up accessibility
Draw the Electronic Security Perimeter

• One or more Electronic ESPs must enclose all identified Critical Cyber Assets

• Spanning geographically separated Critical Assets is not recommended

• Don’t forget!
  – Everything else on the same or subordinate network segments is within the ESP
  – Anything directly connected to a Cyber Asset within an ESP is also within the ESP Perimeter (or is an access point)
Identify the ESP Access Points

• If traffic enters or leaves the ESP, there is an Access Point somewhere:
  – Firewalls
  – Routers
  – Layer 3 switches
  – Layer 2 switches with access control capability
  – Modems
  – Wireless Access Points
  – Dual-homed PCs/Servers
Document... Document... Document!

- Document each Cyber Asset within the ESP
- Document each ESP access point
- Document each Access Control system
- Document each Access Monitoring/Logging System, including those outside the ESP
- Pictures work great at a high level – details needed for completeness
  - For example: IP addresses, model numbers, serial numbers, property tag numbers, system names – unique information
Document Access Control Mechanisms

- Organizational processes and technical/procedural mechanisms that control electronic access must be documented
  - Deny access by default
  - Disable unneeded ports and services
  - Secure dial-up access
  - Strongly authenticate interactive access – at the electronic access point
  - Manage access request and authorization
  - Display acceptable use banners
Monitor and Log Electronic Access

• Monitor and log access at each electronic access point
  – Includes each dial-up access point to a dial-up accessible device

• Detect and alert on attempted or actual unauthorized electronic access
  – Notify appropriate response personnel
  – Promptly evaluate the alert and respond appropriately

• Can’t automatically detect and alert?
  – Review access logs for attempted or actual unauthorized access at least every 90 calendar days

• Keep records
Vulnerability Assessment

• Document the vulnerability assessment process
• Verify only ports and services required for operations at the access points are enabled
  – Access control list/firewall rule set review
• Review controls for default accounts, passwords, network management community strings
  – Verify the controls are implemented and working
• Document results
• Develop remediation/mitigation action plans
• Document the action plan execution status
Review the Documentation

- Review annually and update as necessary:
  - ESP documentation
  - Electronic access controls
  - Electronic and/or manual access monitoring and logging processes
  - Cyber Vulnerability Assessment
    - Don’t forget the documentation supporting the assessment
  - Update documents within 90 days following modification of the network or access controls
  - Keep access logs for 90 days (or three years per CIP-008-3)
Putting It All Together

• Define and document your ESP...and everything in it
• Document your electronic access controls
• Monitor and log all electronic access
• Perform the annual vulnerability assessment
• Perform the annual documentation review
• Most importantly, keep good records
  – Helps you protect your systems
  – Helps you demonstrate compliance