CIP-005 R2: Electronic Access Controls

Knowing who is in your network

Steven Keller
Senior Compliance Specialist – CIP
skeller.re@spp.org · 501.688.1633

September 28, 2012
Objectives

• Improve your understanding of CIP-005 R2
• Share areas of concern and issues of non-compliance we have seen
• Discuss ways you can improve overall security of Critical Cyber Assets
  – Successful practices we have seen during audits
  – Best practices to consider
What are Electronic Access Controls?

• Control access to your environment
• Protect your environment from those on the outside
• Processes or procedures to secure your electronic network from unauthorized access
• Associated configuration and change control process to ensure each access point stays up-to-date
EAC is like a guarded fence with access points
Registered Entities must....

• Develop policies and procedures about your EAC and how it works
• Develop good internal controls for your systems
• Know who accesses your Electronic Security Perimeter and why
• Document and control access
EAC Policies and Procedures

• Policies and Procedures = Internal Controls
  – Always start with a Policy + Management
  – Develop procedure after clear policy is in place
  – Policy supports the rest of what you do
    ▪ What about your Physical Security Perimeter?

• Documentation must cover:
  – How your network is configured
  – All of your access control points
  – Sufficiently detailed network diagram
Deny by Default – R2.1

- Discover your access points (R1)
  - Must know where traffic is entering network to manage/restrict it

- “Build a fortress” with your ESP

- “Deny by Default” means let nothing in or out
  - Start with Deny by Default

- Most people assume it is okay to allow “inside to outside”
  - Should restrict data both ways
Access Points– R2.2

• Prepare to show your access control lists to auditors
  – Include comments

• Document list of open/running ports and services with explanation
  – Vendor’s generic list is not sufficient

• Have you considered all access points?
  – Firewalls - Digiboards
  – Modems - Dual-homed systems
  – VPN servers

• Verify what is documented to what is actually occurring
Say it, prepare to show it!

- SMEs need to explain why ports and services are open
- Must verify that what is written matches what is audited
Real-Life Example

• SME – close to retirement - was very knowledgeable on access points and firewalls

• When we interviewed SME, what he told us was not supported by documentation

• Company needed to get knowledge out of SME’s head and on paper

• This disconnect resulted in “area of concern”
Dial Up – R2.3

• Secure your modems
• Document a procedure on how to secure your dial-up system, even if you don’t have or plan to have one
  – How is dial-up controlled?
  – Does it have dial back?
  – Is the physical connection made?
• Treat your dial-up the same as any other access point
• NERC has called our attention to this
Strong Technical/Procedural Controls – R2.4

• Be prepared to explain your “strong controls”
• How do you know “Steven Keller” really is “Steven Keller” accessing your network?
• You might consider using “two factor” authentication

  Two of the following:
  1. Something you have
  2. Something you know
  3. Something you are
Access Controls Documentation– R2.5

• Documentation should, at least, identify and describe:
  – Process for access request and authorization
  – Your authentication methods
  – How you review your authorization rights
  – Controls used for securing dial-up

• Document, Document, Document
  – Should match what your processes are
  – Give detail how 2.5.1 through 2.5.4 are specifically met
Appropriate Use Banner – R2.6

- Banner is like “Do Not Trespass” sign: Only authorized users are allowed
- Banner documentation must match your banner
- Banner must appear before user attempts to log in
- Unable to display a banner? Apply for a TFE
Real-life Violations – Banner Use

1. Banner capability not implemented at substation and no documentation of required banner
2. No documentation identifying banner that is displayed on login to the asset
3. Two ESP Access Point devices display banners that do not comport with documented banner language
4. Firewall doesn’t display banner until user has logged in – and there was no TFE
Best practices we have seen

• Spreadsheet including active ports, why they are active, software used
• Documented services associated with active ports
• Restricted inbound and outbound traffic
• Restricted traffic to specific host IP addresses
• Defined process to validate need for new port

Resources:

Compliance Analysis Report CIP-005
Current draft CIP-005-5 Guidance Section
Questions and Summary

- Good documentation demonstrates your EAC is effective and well-maintained.
- Make sure someone not familiar with your company could understand your EAC.
- Ports and Services should be well documented by you - not your vendor.
- Have a documented dial-up procedure, even if you do not allow it.
- Document your authentication methods to request and receive access.
- Have and document your appropriate use banner.
- Implement what you have documented!
CIP Team

Kevin Perry, Director of Critical Infrastructure Protection, (501) 614-3251

Shon Austin, Senior Compliance Specialist-CIP, (501) 614-3273

Steven Keller, Senior Compliance Specialist-CIP, (501) 688-1633

Leesa Oakes, Compliance Specialist II-CIP, (501) 614-3274

Jeremy Withers, Compliance Specialist II-CIP, (501) 688-1676
Upcoming Events

Bookmark the RE Calendar and Events page to see all scheduled events at a glance

• **Fall Compliance Workshop**, Nov. 13-14, Little Rock. [Agenda](#)

• **2013 Implementation Plan and Audit Scope** webinar, Dec. 3, 2:00

• **CIP-003-3 R5 Controlling Access to CCA Info** webinar, Dec. 12, 10:00

• **RE Trustee Meetings**
  - **October 29, 2012** – Little Rock
  - **January 28, 2013** - New Orleans
  - **April 29, 2013** - Kansas City
  - **July 29, 2013** - Denver
  - **October 29, 2013** - Dallas
Check out our new training videos!

vimeopro.com/sppre/basics

Navigate there from SPP.org>RE dropdown>Training & Education

COMPLIANCE AND ENFORCEMENT: THE BASICS