Adequate CIP Evidence

Patrick C Miller, President and CEO, EnergySec

August 09 2011

Utility Information Technology (UNITE)

Authority

- Per 18CFR39, FERC, NERC and the Regions have the direct and delegated authority to ask for nearly anything… *and you are required to provide it*

- If you don't, their easiest path is to write up a violation for insufficient (or lack of) evidence and then it is all up to the lawyers

Evidence Presentation

- Goal is to simplify the auditor's search
- Minimize the "Columbus Method"
- Use the RSAW to your advantage
  - Point to exact page, paragraph of document
  - Electronically highlight if possible
- Connect the dots in advance for the auditor
- Parent and child documents
- Stub-referencing is fine, but it must be accurate

Evidence Presentation

- Redaction is allowed, but only where appropriate
  - Use this only when you really don't want to provide the full document
  - Don't go overboard
  - When in doubt, ask
- Human readable
  - Here it is, but you will need *[insert proprietary product X]* to read it
- Avoid reflexive reference of the standard

Look And Feel

- Classification (don't violate CIP-003.R4)
- Header, footer
- Date created
- Revision block
- Signature block
- Sectioning, numbering
- Location/placement of elements
- General formatting: font, size, etc

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the US Department of Energy

Evidence Types

- What type of evidence is best?
  - Yes. Yes it is.
  - No, really…
    - Word, Visio, Excel, PDF
    - System/event logs
    - Database reports
    - Observations
    - Pretty much anything

Quality, Not Quantity

- Concise, direct, brief, compact…
- Avoid "dumptrucking"
  - 1T of data will not help your situation
  - Can't find it = no evidence provided
- Documents MUST be searchable
  - Get familiar with your OCR
- Auditors use "triangulation"
  - Three points equals a hit

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the US Department of Energy

Know Your Stuff

- Know the standard
- Know your evidence
- Know your SMEs (know your people)
- Know your policies
- Know where else to look
- Know your audit team
- Don't be afraid to ask for clarification

Automate^3

- Manual evidence is very hard to maintain
- Log everything you possibly can to build base
  - Be mindful of performance hits
- But first… nail your business process
  - Automating bad process means you will just fail faster and more accurately
- Automation requires care and feeding too
- Continuous monitoring

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the US Department of Energy

Maintenance

- Again, manual evidence is **hard to maintain**
- Humans are prone to error, vacation, malice…
- Entropy is working against you
- Maintain few systems of record for source data
- Maintain single store (digest) for reference, but pull all data from sources
- Automate aggregation, parsing, alerting…
- Dashboards

Critical Cyber Asset Data

- CIP-003.R4 does not equal Critical Cyber Asset
- Yes, data can be a CCA, but rarely so
- Adhere to CIP-003.R4 and CIP-003.R5 classification restrictions on all relevant systems
- CIP evidence is top target for attackers
  - Protect evidence stores with additional security

Evidence Retention

- FIRST: *Check with your legal department before deciding how long to keep or when to destroy*
- Required retention period varies by Region
  - Some only ask for one year
  - Some ask for all data back to prior audit
- Keep all data since last audit
- Use appropriate destruction methods

Third Party Evidence

- Ultimately, you, the Registered Entity are on the hook for providing evidence
- Third party may store/maintain evidence
  - Consider a 24-48 hour provision clause in contract
  - Test to ensure expected content is provided in expected timeframe
  - Alert third parties before audit to prepare them

Example One: CIP-003.R1.2

- *The Cyber Security policy is available to all personnel who have access or are responsible for Critical Cyber Assets*
- Commonly evidenced by:
  - URL and screenshot of corporate intranet site
  - Email or change record noting date of post to site
  - Copies of print material used where electronic access is unavailable
  - Policy statements referencing availability of the policy

Example Two: CIP-004.R2.1

- *This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization*
- Commonly evidenced by training [attendance] logs
  - For all respective personnel
  - Contain date of authorization **and** date of training
  - Can be extract from database or sign-in sheet

Questions?

Non-profit. Independent. Trusted.

Patrick C Miller, President and CEO
patrick@energysec.org
503-446-1212
@PatrickCMiller

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the US Department of Energy