What is "CONNECT"™?

Did you know that RFL has been serving the Power Utility industry for over 50 years? Did you also know that RFL has been serving customers since 1922?

Over all this time, RFL has amassed a tremendous amount of industry knowledge and expertise, which we want to share with you, our valued customers, and thus, CONNECT™, a learning center for the Power Utilities, was developed.

CONNECT™ training and seminar topics include Networking, Communications, Protection and Cyber Security. Future topics will be designed around issues that are relevant to the Power Utilities.

All CONNECT™ seminars are complimentary because RFL wants to stay CONNECTED with its customers by offering products and services that are meaningful and valuable.

Please visit RFL's web site to register and see the latest syllabuses and training schedules at www.rflelect.com.

RFL CONNECT™
Learning Center for Power Utilities

Module 5:
Documentation and Evidence of Compliance/NERC CIP

Prepared by RFL Management Team
January 8, 2015
Karl Perman

ENERGYSEC
SERVING THE INDUSTRY'S SECURITY COMMUNITY SINCE 2004

Agenda

1. Documentation
2. Measures
3. Evidence
4. Tips for Success

Documentation

- Can be from manual or automated sources
- Documentation still needed for audit
- Examples are provided in the measures section

Documentation Examples

- BES Cyber System Identification Process
- Cybersecurity Policies
- Security Awareness
- Security Training
- Personnel Risk Assessment
- Access Management
- Electronic Security Perimeters
- Physical Security Plan
- Patch Management
- Malicious Code Management
- Incident Response
- System Recovery
- Configuration Management
- Vulnerability Assessments
- Information Protection

Measures

- Exist in both root requirements and tables (CIP-004 – CIP-011)
- Each requirement part has an associated measure
- Measures are worded as suggestions
- Measures provide examples of what might constitute acceptable evidence
- Not comprehensive
- Not authoritative

Measures: Example

Measures
An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Measures: Example

CIP-003

- *examples of evidence may include … revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months*

- requires actions to be taken to demonstrate compliance

Measures: Example

- CIP-004
- *Dated copies of information used to reinforce security awareness, as well as evidence of distribution*
- Actual materials distributed, to demonstrate compliance

Measures: Example

- CIP-007
- *Configuration files of host- based firewalls or other device level mechanisms that only allow needed ports and deny all others*
- Backing up procedures with actual copies of device configurations is a great way to demonstrate compliance with technical requirements

Evidence

Evidence is simply a collection of artifacts that demonstrate your compliance with the underlying requirements.

- program documentation,
- system logs,
- email records,
- interviews,
- observation,
- database records, and
- many other items

Evidence and Auditors

- Auditors are “independent” and may not “stick to the script”
- Auditors are obligated to “obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions”
- Evidence stacking

Evidence Retention

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

Tips for Success

- Establish what will be required to demonstrate compliance by requirement
- Assign ownership for evidence
- Create awareness of “evidence”
- Maintain a central repository for all evidence
- Implement a review process to ensure documentation meets evidence standard
- Publish metrics so stakeholders are aware of areas of concern
- Be cognizant of information protection procedure

Questions?

Karl Perman
karl@energysec.org
503.905.2920 Ext. 310
www.energysec.org

Next Module…

Module 6: Bright Lines and System Categorization Part One

This module provides an introduction of bright line criteria, cyber asset identification and BES Cyber Asset/System Categorization.

January 15, 2015