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

Communication Networks Part 1

Agenda

- Fundamental Definitions
- Overview of Routable Communication Networks
- External Routable Connectivity
- CIP Requirements and External Routable Connectivity
- Final Thoughts
- Questions

Fundamental Definitions

- **Cyber Asset**: Programmable electronic devices, including the hardware, software, and data in those devices.

- **BES Cyber Asset**: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

- **BES Cyber System**: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Fundamental Definitions

- **Protected Cyber Asset**: One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

- **Electronic Access Point**: A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

- **Electronic Security Perimeter**: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Overview of Routable Communication Networks

Design Considerations

- Identify networks to which BES Cyber Systems are connected via a routable protocol
- Identify BES Cyber Systems connected to each network or network segment
- Determine which BES Cyber Systems and associated Protected Cyber Assets you want to segment
- Put in EAPs to separate the ESPs
- Consider perimeter protection for each EAP

Dial-Up Connectivity

- A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link
- This includes outbound connections
- All dial-up connectivity must be protected by authentication, except where it is not technically feasible

Communications Network

- No clear, general definition
- Sometimes used to mean:
- Wiring and other transport media, or
- Broader collection of network equipment and supporting devices

Network Devices

- Routers, switches, firewalls, and other networking equipment which directly supports ESP networks are in-scope and have requirements

CIP REQUIREMENTS AND EXTERNAL ROUTABLE CONNECTIVITY

Standards Affected by ERC

Training and Awareness	CIP-004-5 R1 and R2
Personnel Risk Assessments	CIP-004-5 R3
Access Management	CIP-004-5 R4 and R5
Electronic Security Perimeters	CIP-005-5 R1
Interactive Remote Access	CIP-005-5 R2
Physical Security	CIP-006-5 R1, R2 and R3
Ports and Services	CIP-007-5 R1
Security Event Monitoring	CIP-007-5 R4
System Access Control	CIP-007-5 R5

Training & Awareness

- Medium Impact w/ ERC and w/o ERC must:
  - Provide security awareness training each quarter
- Medium Impact w/ ERC has requirements on
  - Specific topics to be covered
    - Cyber security policies, physical/electronic access controls, visitor control program, handling of BES Cyber System Information, identification of and response to Cyber Security Incidents, recovery plans, cyber security risks associated with a BES Cyber Systems electronic interconnectivity and interoperability with other Cyber Assets
  - Training must be completed prior to granting access
  - Must train every 15 months

Personal Risk Assessments

- Medium Impact w/ ERC has requirements, w/o ERC has no requirements
- Requirements:
  - Process to confirm identity
  - Perform a seven year criminal history records check
  - Criteria or process to evaluate criminal history records checks
  - Verify contractors or service vendors have personnel risk assessments performed
  - Risk assessments are performed at least every 7 years

Access Management

- Medium Impact w/ ERC has requirements, w/o ERC has no requirements
- Requirements:
  - Process to authorize access based on need
  - Verify each quarter that individuals with access have authorization records
  - For electronic access, verify every 15 months that user accounts, user account groups, or user role categories and their privileges are correct and necessary
  - Every 15 months, verify that access to storage locations for Cyber System Information are correct and necessary

Access Management Revocation

- Medium Impact w/ ERC has requirements, w/o ERC has no requirements
- Requirements:
  - Remove access authorization upon a termination action within 24 hours of the termination action
  - Remove access authorization upon reassignment or job transfer by the end of the next calendar day
  - For termination actions, revoke access to Cyber System Information by the end of the next calendar day

Electronic Security Parameters

- Medium Impact w/ ERC
  - All External Routable Connectivity must be through an identified Electronic Access Point
  - Perform authentication when establishing Dial-up Connectivity, if technically feasible
- Access Points
  - Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default
- Access Points at Control Centers
  - Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications

Interactive Remote Access

- Only Medium Impact w/ ERC has requirements
- Must use an Intermediate System
- Utilize encryption that terminates at an Intermediate System
- Require multi-factor authentication for all IRA sessions

Physical Security

- Medium Impact w/o ERC and Physical Access Control Systems (PACS) associated with Medium Impact w/ ERC must have operational or procedural controls to restrict physical access
- PACS associated with Medium Impact w/ ERC must monitor for unauthorized access, issue an alarm for unauthorized access, and test the equipment every 24 months

Physical Security

- Medium Impact w/ ERC must:
  - Use at least one physical access control
  - Monitor for and raise an alarm in response to unauthorized access
  - Log entry of each individual with authorized unescorted physical access
    - Identify the individual and the date and time of entry
  - Provide continuous escorted access for visitors
  - Log entry of visitors
    - Include name, date and time, and name of an individual point of contact responsible for the visitor
    - A single record for the entire day is allowed, even with exit and re-entry
  - Retain both sets of access logs for at least 90 days

Ports and Services

- Medium Impact w/ ERC must
  - Have documented procedure for determining which network accessible ports are required
    - Can use port ranges to handle dynamic ports
  - Only required ports may be enabled
  - Must be on the local machine
  - Can be accomplished using host-based firewall

Security Event Monitoring

- Medium Impact w/ ERC must generate alerts for security events
- Events that must generate alerts:
  - Detected malicious code
  - Detected failure of logging
  - Additional events to meet the intent of the requirement
- Suggested events that raise alerts:
  - Login failures for critical accounts
  - Interactive login of system accounts
  - Enabling of accounts
  - Newly provisioned accounts
  - System administration or change tasks by an unauthorized user
  - Authentication attempts on certain accounts during non-business hours
  - Unauthorized configuration changes
  - Insertion of removable media in violation of a policy

System Access Control

- Medium Impact w/ ERC or Medium Impact w/o ERC but at Control Centers must have a method to authenticate interactive user access
- Medium Impact w/ ERC must:
  - Identify individuals who have authorized access to shared accounts
  - For password-only authentication for interactive user access, either technically or procedurally enforce password changes at least once every 15 months

Caution

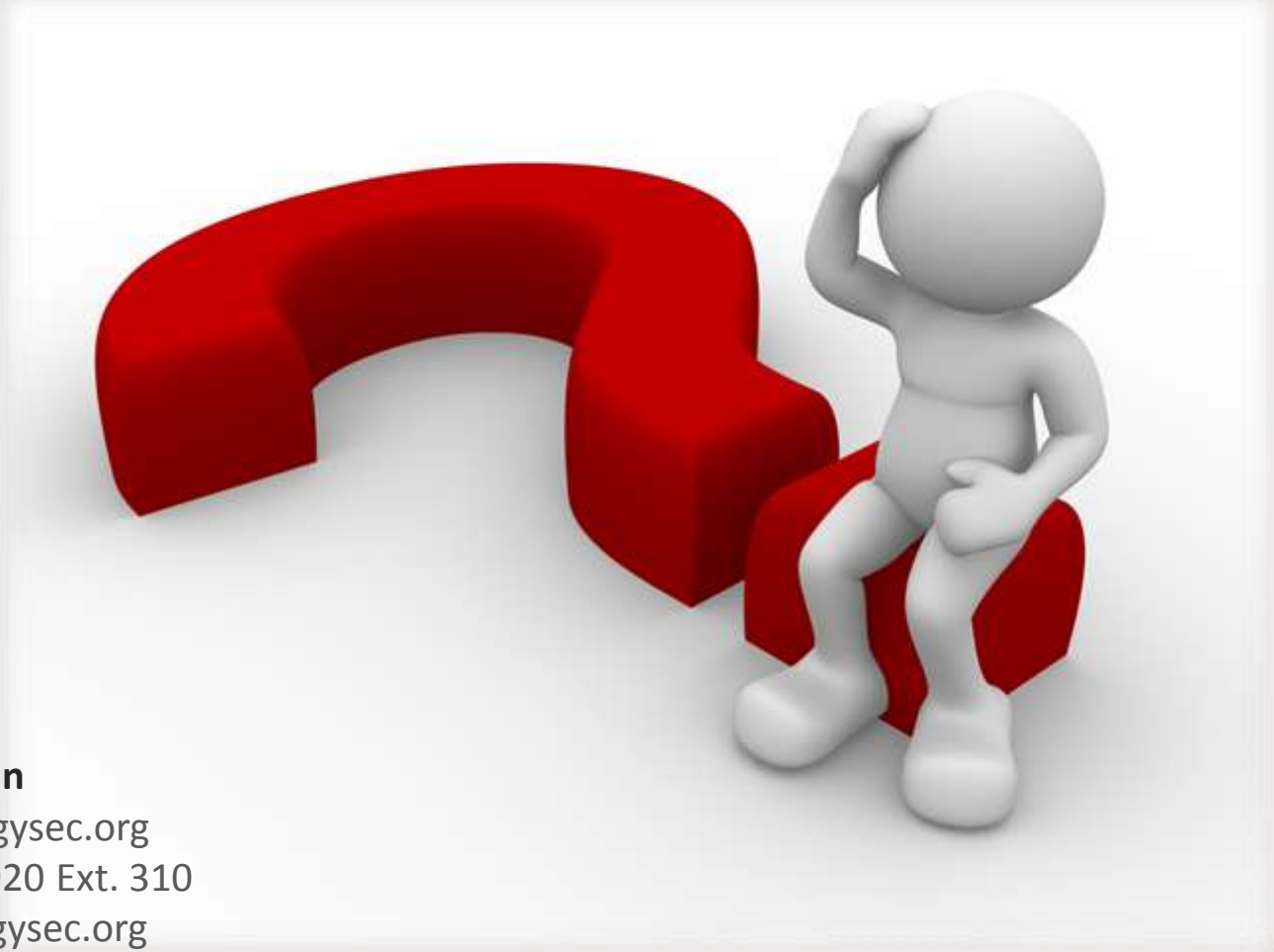
- A change in communication levels could bring many new requirements into scope for an asset and cause an immediate violation
- This would happen immediately because there is no provision in the CIP-002 identification process to distinguish ERC and non-ERC assets

FINAL THOUGHTS

Final Thoughts

- Need to be familiar with definitions
- External Routable Connectivity introduces many more CIP requirements for the BES Cyber Assets
- All External Routable Connectivity must be through an External Access Point

Questions?



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