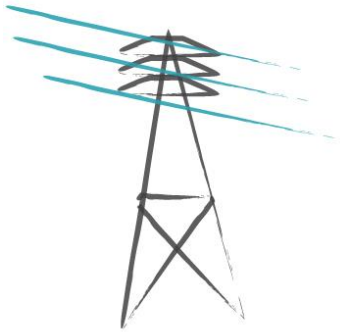


WECC

# Applicability of Communication Networks

## Compliance Workshop November 14, 2017

Eric Weston

Auditor, Cyber Security

# Reliability Impact Statement

Communication and networking Cyber Assets that provide communications can be challenging to classify due to the inherent nature of their failure impacting critical communications.

# Communications Protections

- CIP-005 Electronic Security Perimeters (ESP) and Electronic Access Points (EAP)
- CIP-006 Part 1.10 communication link protections between extended ESPs
- CIP-012 Data transmitted between Control Centers

# Electronic Security Perimeter

# Electronic Security Perimeters

## Basics of an ESP

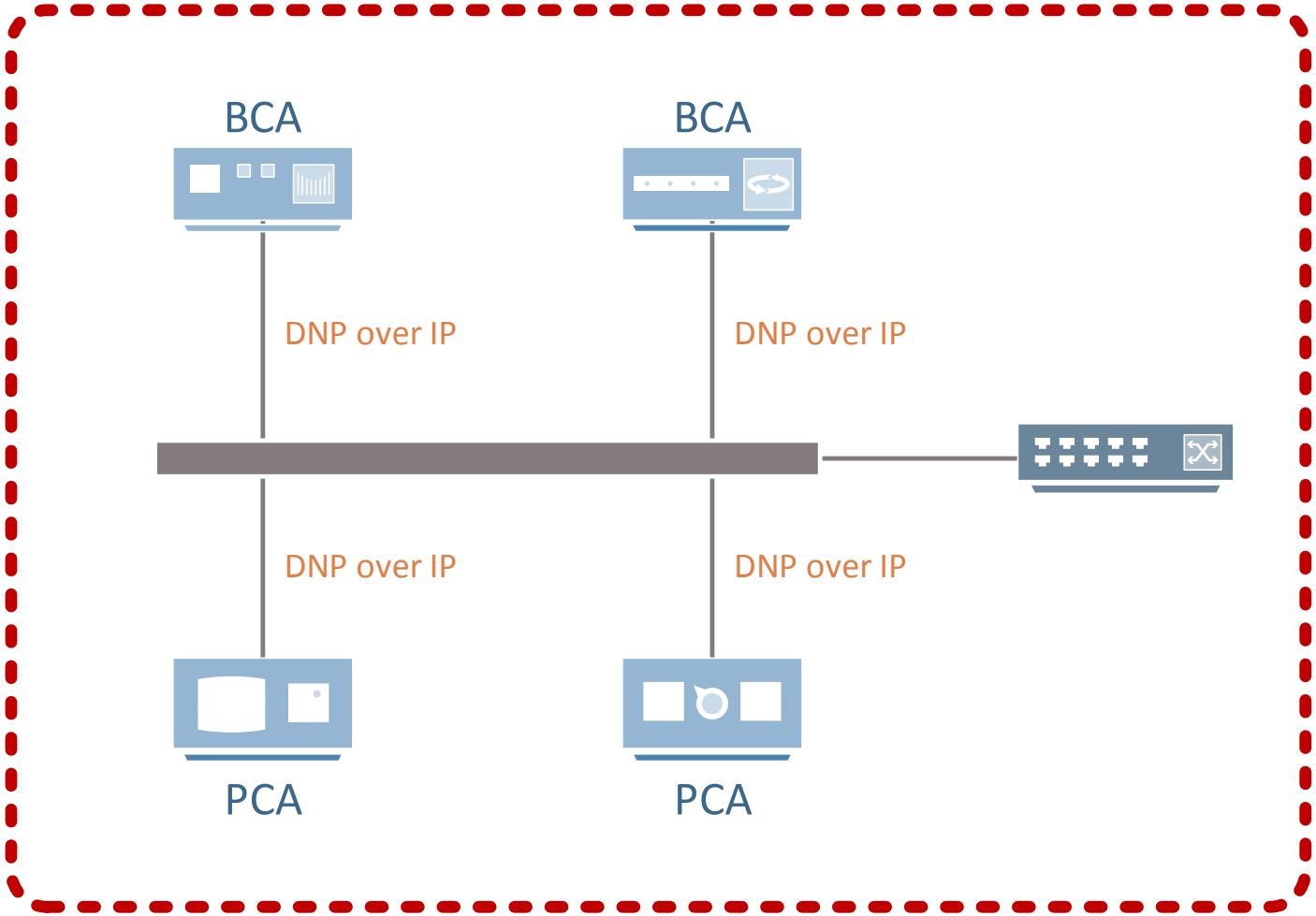
- Logical border around BES Cyber Systems
- Devices are connected using a Routable Protocol
- All External Routable Connectivity (ERC) must be through an identified EAP
- The EAP provides protections for the network and devices within

# Electronic Security Perimeters

## An ESP without ERC

- BES Cyber Systems connected using any routable protocol need to be within an identified ESP regardless of the presence of ERC
- Island ESPs
- ESPs are the basis for identifying potential PCAs

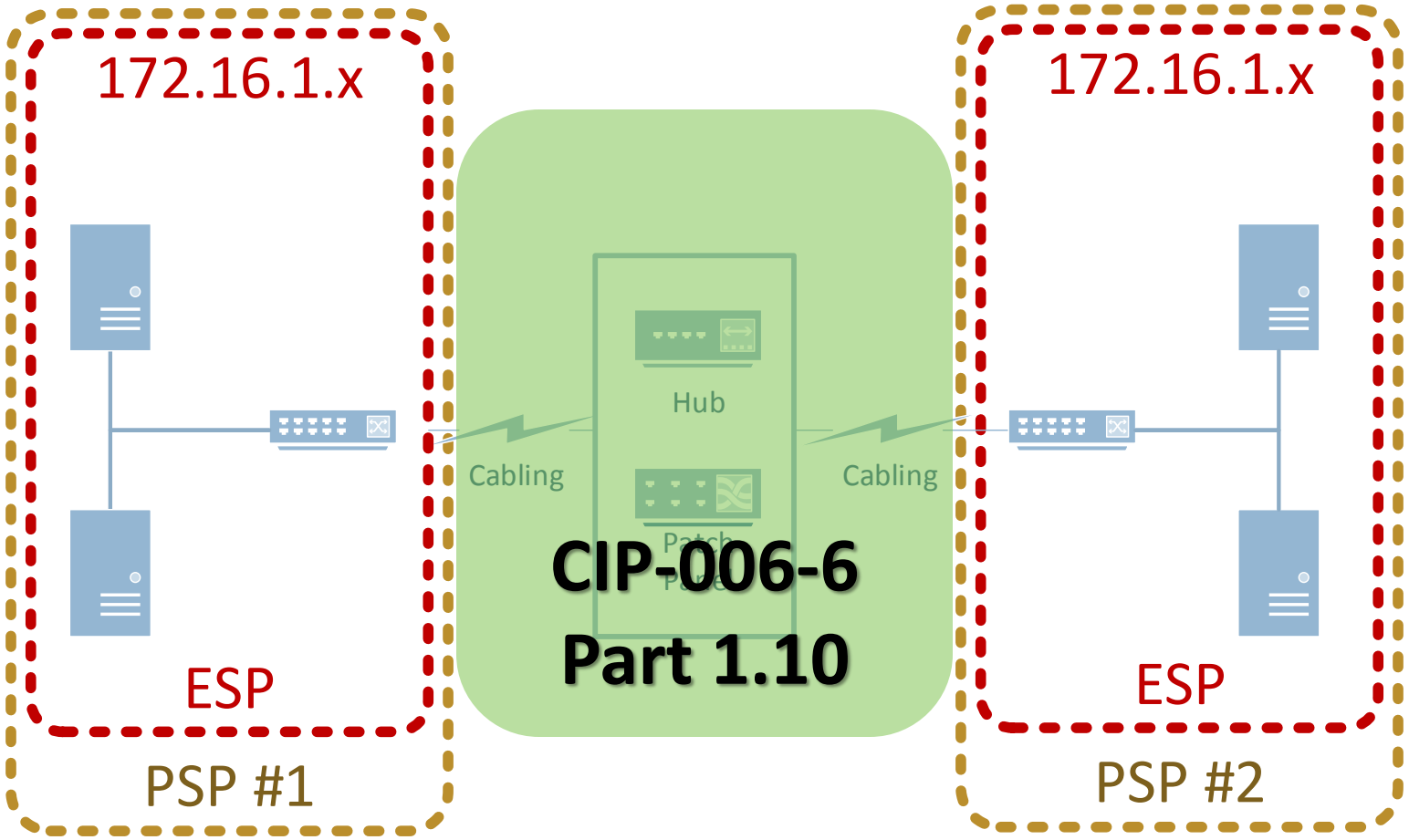
# Electronic Security Perimeters




Identified ESP with no ERC

# CIP-006-6 Part 1.10

# Physical Protection of Communications Equipment and Cabling CIP-006-6 Part 1.10




Extended ESP

# Physical Protection of Communications Equipment and Cabling CIP-006-6 Part 1.10

- Types of equipment to watch out for outside the Physical Security Perimeter (PSP):
  - *Cabling*
  - *Unmanaged switches*
  - *Hubs*
  - *Patch panels*
  - *Media Converters*
  - *Couplers*
  - *Port Savers*

# Physical Protection of Communications Equipment and Cabling CIP-006-6 Part 1.10

- What we are looking for during audit
  - Equipment and Cabling should be identified and documented
  - Protections should be identified
  - If encryption is the method used for Part 1.10 protections, please provide evidence of the encryption implementation
  - Be prepared to demonstrate protections during site-visits

# CIP-012-1

# CIP-012-1
# Communications between Control Centers

# Communications and Networking Lessons Learned

# Communications and Networking Lessons Learned

- CIP-002-5.1a: Communications and Networking Cyber Assets[1]
  - Published October 6, 2015
  - Guidance on determining the communications and networking Cyber Assets that should be **in scope** of the CIP v5 Standards
  - Provides generic examples for categorizing network and communication devices

[1] http://www.nerc.com/pa/CI/tpv5impmntnstdy/Communications%20Networking%20Lesson%20Learned.pdf

# Communications and Networking Lessons Learned

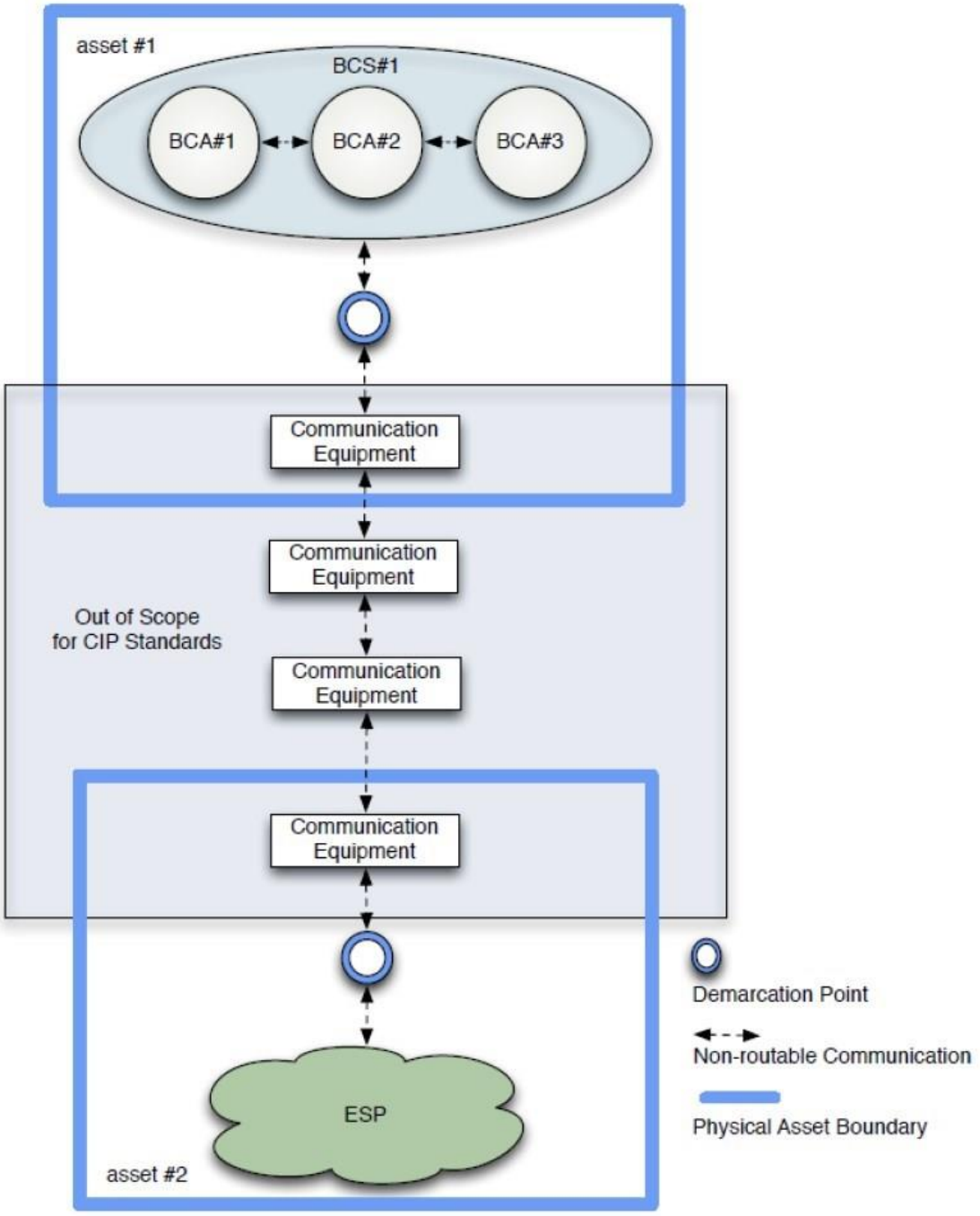
How should this Lesson Learned be used?

- Guidance for ensuring network and communication devices are identified and categorized correctly
- Not meant to provide loopholes for excluding devices from CIP Compliance

# Communications and Networking Lessons Learned

Concepts introduced in the Lesson Learned

- Demarcation points
  - Not a defined term
  - May be confused with common telecommunications terminology
- External communications
  - Not a defined term
  - Lesson Learned does not specify if communications is external from a device or a network




http://www.nerc.com/pa/CI/tpv5impmntnstdy/Communications%20Networking%20Lesson%20Learned.pdf

# Wrap up

- Ensure all BCAs connected with a routable protocol reside within an identified ESP
- For extended ESPs, ensure all nonprogrammable communication components are protected
- Stay informed with developments of CIP-012-1
- Ensure communications devices are identified and protected appropriately

# Questions & Contact Information

Eric Weston
(801) 819-7630
eweston@wecc.biz