NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Lesson Learned
# CIP Version 5 Transition Program
## CIP-002-5.1: Communications and Networking Cyber Assets

Version: October 6, 2015

Authorized by the Standards Committee on October 29, 2015 for posting as a supporting reference pursuant to section 11 of the Standard Processes Manual.

*This document is designed to convey lessons learned from NERC's various CIP version 5 transition activities. It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.*

### Purpose

The purpose of this Lesson Learned is to provide guidance on the categorization of Cyber Assets associated with communication and networking for BES Cyber Systems and includes some sample approaches. In the absence of a defined Electronic Security Perimeter (ESP), the Registered Entity needs to determine the communication and networking Cyber Assets that are in scope of the CIP version 5 Reliability Standards.

### Background

In version 3 of the CIP Standards, the ESP construct provides a demarcation point for Cyber Assets in scope. Cyber Assets external to the ESP are clearly out of scope under CIP version 3, and the applicability section for each CIP version 3 Standard includes an exemption for "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." The same exemption is included in Version 5 of the CIP Standards, but now BES Cyber Systems may not have a defined ESP. In addition, the Version 5 Standards can include communication and networking Cyber Assets that are included in scope as BES Cyber Assets(BCA) or Protected Cyber Assets (PCA).

Reliability Standard CIP-002-5 Requirement R1 Attachment 1 requires Responsible Entities to identify high and medium impact BES Cyber Systems and assets that contain a low impact BES Cyber System. This identification is based on impacts to the reliability tasks performed at assets such as Control Centers, generation facilities, and transmission facilities. Communication and networking Cyber Assets that provide external communications can be challenging to classify due to the inherent nature of a single point of failure impacting external communications. The Cyber Assets that are necessary for external communications, with or without an ESP, should be treated the same for exclusion in the CIP version 5 Reliability Standards.

For high and medium impact BES Cyber Systems with a defined ESP, classification of network devices is less of an issue because such devices are clearly either (i) out of scope or (ii) identified as a BCA , or (iii) identified as PCA, which receive a commensurate level of protection as a BCA.

In general, network devices do not perform application logic of the reliability function, but certain network devices may be a necessary component in the workings of the BES Cyber System. This Lesson Learned presents approaches used by Implementation Study[1] participants to categorize network devices associated with high and medium impact BES Cyber Systems.

## Guidance

Examples of the approaches taken by study participants are described below. The classification of communication and networking devices is described as well as several diagrams to show some examples of the approaches taken.

### *Network Devices Classified as BES Cyber Assets*

As the study participants evaluated the reliability tasks performed at each asset, participants recognized that certain network and communication devices should be categorized as BES Cyber Assets. The determination was based on the assessment that if the network devices were rendered unavailable, degraded or misued they would have the potential to adversely impact the reliable operation of the asset. One example was a network device providing backbone communication for the local BES Cyber System. Another example of this network device might be a core switch passing traffic between devices on a plant control network or substation network. In contrast, the communication and networking devices that were only being used for external communications did not have an impact on the reliability tasks performed at the asset and, in turn, were not classified as BES Cyber Assets.

### *Network Devices Classifed as Protected Cyber Assets*

The study participants also recognized that certain network devices, while not identified as a BES Cyber Asset, would meet the definition of a Protected Cyber Asset (PCA). Specifically, network devices may reside on the same local, routably connected networks as BES Cyber Systems but would not meet the definition of a BES Cyber Asset because if the network device were rendered unavailable, degraded or misused, it would not have the potential to adversely impact the asset. For example, a network device might be a network switch added to create a way to gather all the event data from multiple devices into a single device for analysis at a future time. Because the network devices have a routable connection to a BES Cyber System and was included inside the ESP by the participants, the network device was categorized as a Protected Cyber Asset associated with the medium impact BES Cyber System.

## Examples

[1] Ref. Implementation Study Final Report http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf

To show the approaches taken by the study participants, three generic examples are presented below to demonstrate how they categorized network and communication devices associated with high and medium impact BES Cyber Systems. In all three examples, the communication equipment identified is any equipment installed to facilitate external communications. The concept of a demarcation point was used to help determine the communication equipment that was excluded from NERC CIP compliance. The demarcation point was not a requirement for the NERC CIP version 5 Reliability Standards, but provided an approach that was able to be applied with or without a defined Electronic Security Perimeter (ESP). The demarcation point was a physical location chosen by the entity that separated the equipment used for external communications from the equipment that would typically be included in an ESP.

### *Communication and Networking Devices between defined ESP's*

In the first example, shown in Figure 1, the study participant identified the ESP at asset #1, which communicates to cyber assets within an ESP at asset #2 using a routable protocol. Since the ESP at asset #1 has a routable communication outside the ESP, the study participant identified an Electronic Access Point (EAP). After the EAP was established, a demarcation point was established to identify all the communication and networking equipment that was out of scope for the CIP standards (the demarcation point can be located on cabling or a device between the BCS and communication equipment). In this example, the EAP and demarcation point could be the same point, but the demarcation point was shown separately to help demonstrate the similar approach taken in the other examples. The demarcation point was not required for the CIP Standards, but was an approach for scoping the communication systems that were out of scope in the other examples when there is no EAP required in the CIP version 5 Reliability Standards. The communication equipment that is out of scope is the equipment used for establishing external communications at any location.

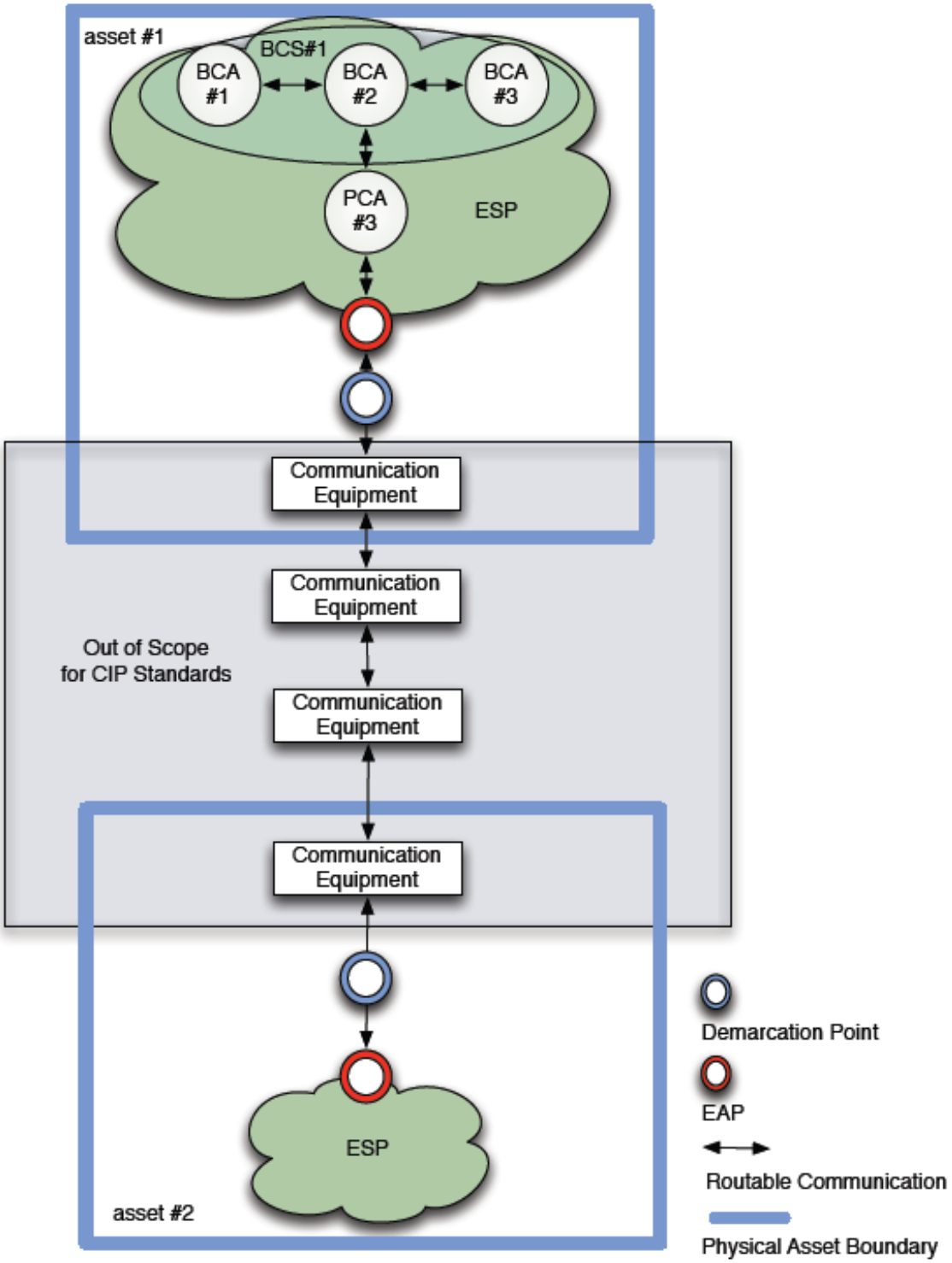
asset #1
BCS#1
BCA #1
BCA #2
BCA #3
PCA #3
ESP
Communication Equipment
Communication Equipment
Out of Scope for CIP Standards
Communication Equipment
Communication Equipment
ESP
asset #2
Demarcation Point
EAP
Routable Communication
Physical Asset Boundary

Figure 1

### *Communication and Networking Devices between an ESP and No ESP*

In Figure 2, the study participant has determined that asset #1 had no local routably connected BES Cyber Assets. The external communications is a non-routable connection to asset #2. Since there were no routable connections, BES Cyber System #1 at asset #1 did not require an ESP or EAP. The communication equipment shown is the same type of equipment used in the first example to establish external communications. The participant established a demarcation point that was between the BES Cyber System and the communication equipment used for external communications (the demarcation point can be located on cabling or a device between the BCS and communication equipment). The communication equipment is out of scope just like the equipment that was out of scope as if there was an ESP at asset #1.

Additionally, asset #2 did have BES Cyber Assets connected using routable communications that were local to the asset. Even though an ESP needs to be established, there is no required EAP since the communications outside the ESP is non routable communications. The demarcation point in this case can be established in the same way as the first example as if there was an EAP on the ESP. The communication equipment considered out of scope is the same communication equipment that would be considered out of scope between two ESP's.

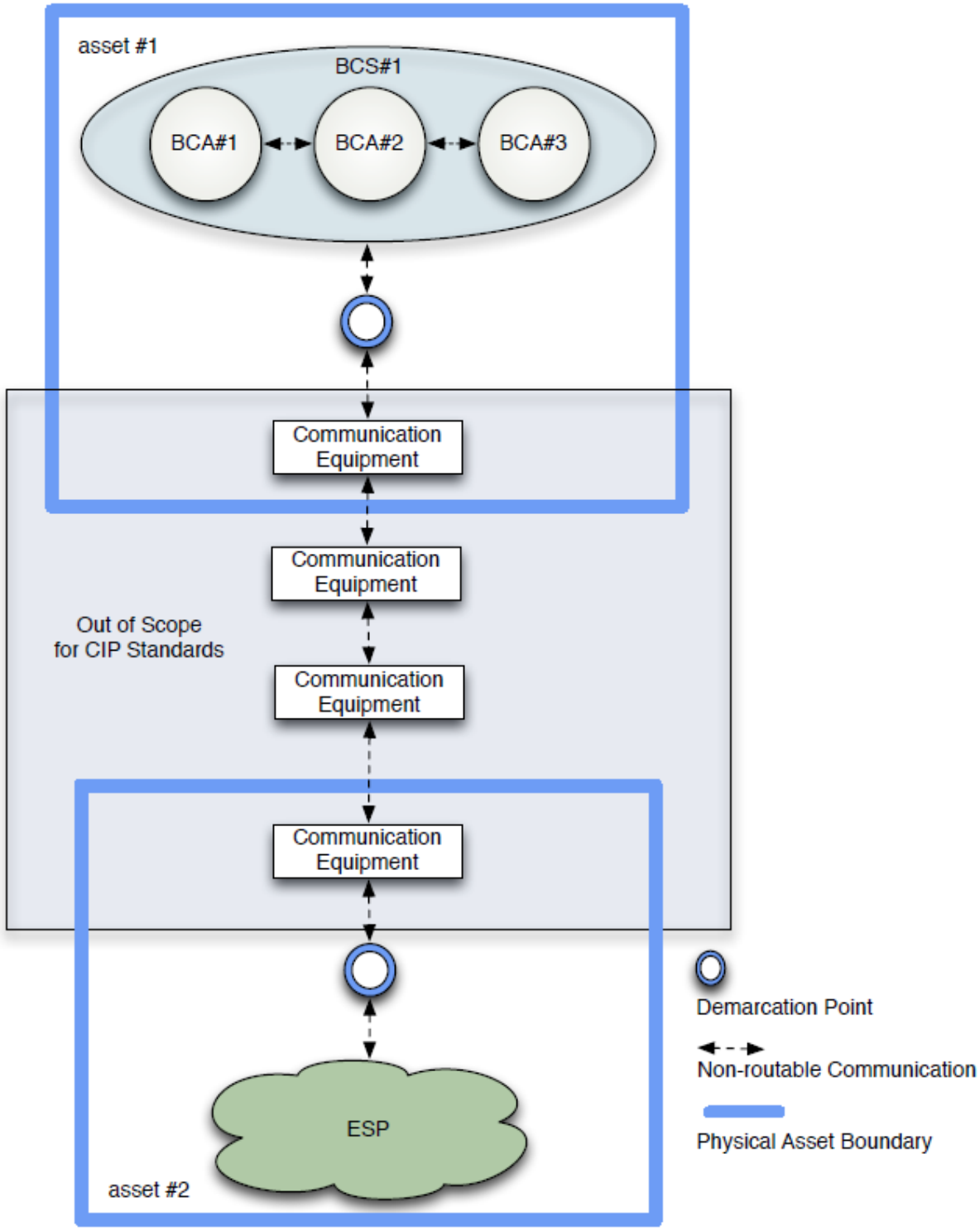
asset #1
BCS#1
BCA#1
BCA#2
BCA#3
Communication Equipment
Communication Equipment
Out of Scope for CIP Standards
Communication Equipment
Communication Equipment
ESP
asset #2
Demarcation Point
Non-routable Communication
Physical Asset Boundary

Figure 2

### *No ESP's Identified*

In this last example shown in Figure 3, the same approach was applied as in the two previous examples. In this case, there were no ESP's identified at asset #1 or asset #2, but there is still communication equipment used for external non-routable communications between the two assets. Since there are no ESP's or EAP's defined, it is very difficult to determine the demarcation point for communication equipment that is out of scope. By establishing a demarcation point (the demarcation point can be located on cabling or a device between the BCS and communication equipment) the same way as the two previous examples, the participant was able to identify the communication equipment that was used for external communications and was out of scope for the NERC CIP version 5 Reliability Standards. Since the same type of communication equipment is out of scope between two ESP's, the equipment was considered to be out of scope when no ESP's were required for the NERC CIP V5 Standards.

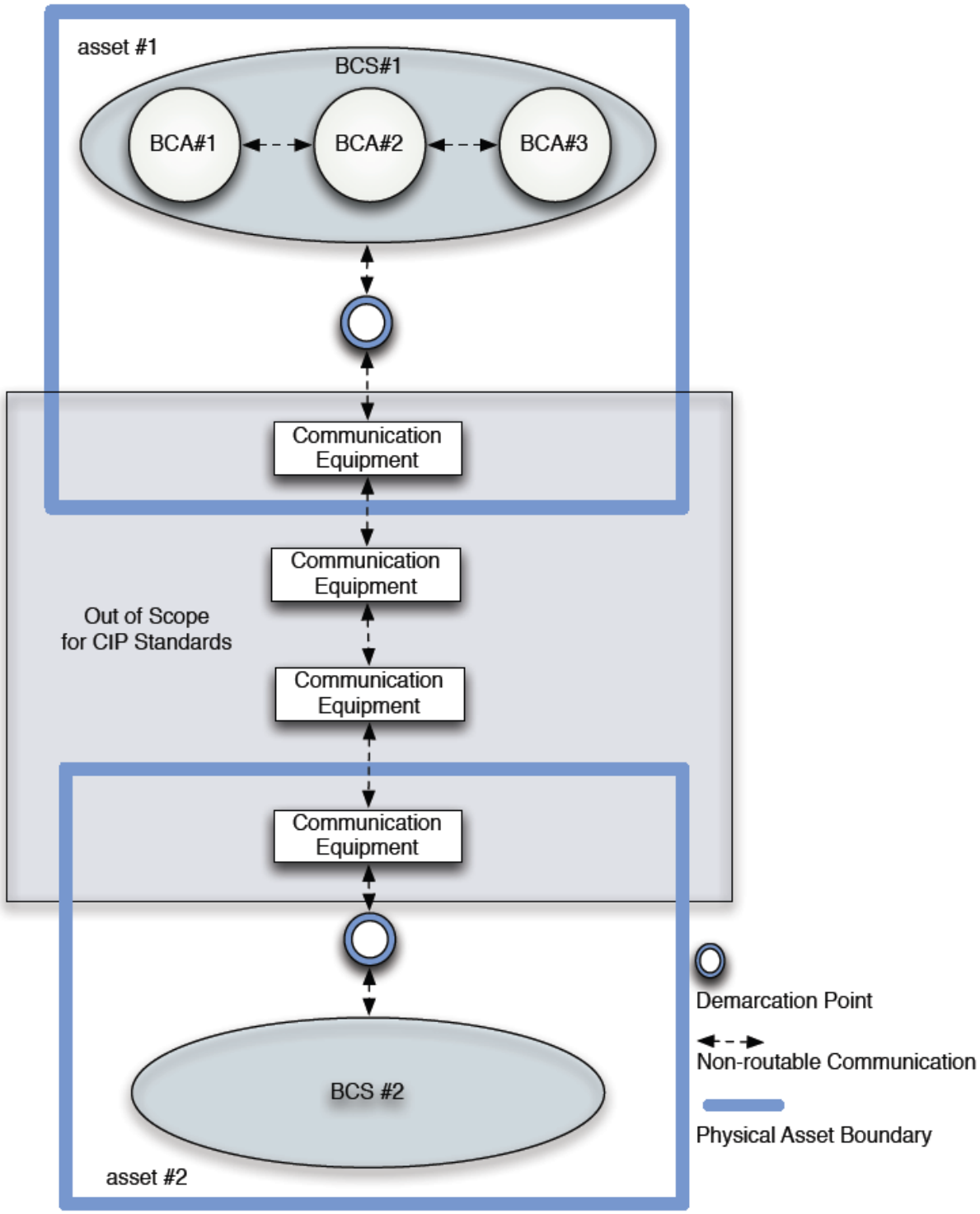
asset #1
BCS#1
BCA#1
BCA#2
BCA#3
Communication Equipment
Communication Equipment
Out of Scope for CIP Standards
Communication Equipment
Communication Equipment
BCS #2
asset #2
Demarcation Point
Non-routable Communication
Physical Asset Boundary

Figure 3

### *Demarcation Point for Network Devices and Communication Equipment Out of Scope*

For the three examples, study participants made a distinction between devices facilitating network communication locally for the BES Cyber Systems and those facilitating network communication external to the BES Cyber System or Facility. Entities determined network devices used only for external communication were out of scope in association with the high or medium impact BES Cyber System. The demarcation point was identified as a physical point between the Cyber Assets identified for external communications and the local BES Cyber Systems. The demarcation point can be located on cabling, a port on a device, a terminal block, or some other device or location determined by the Entity between the BCS and communication equipment.

## Relevant NERC Glossary Terms

**Cyber Assets** – 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. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, A Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

**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.

**Protected Cyber Assets –** 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 Security Perimeter (ESP)** – The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

**Electronic Access Point (EAP)** – 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.