NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

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

Draft Version: August 18, 2015

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, to modify the requirements in any existing reliability standards, nor 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-005-5 Attachment 1 requires Responsible Entities to classify BES Cyber Assets based on their 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 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 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.

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

Examples

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. 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.

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 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.

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 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.

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 basis for exclusion is the unavailability, degredation or misuse of the external communications does not adversely impact the local functioning of the BES Cyber System. It may be countered that loss of external communication prevents the remote control or data acquisition for the Facility, and while true, the reliability impact for remote control or data acquisition is not associated to the high or medium impact BES Cyber System.

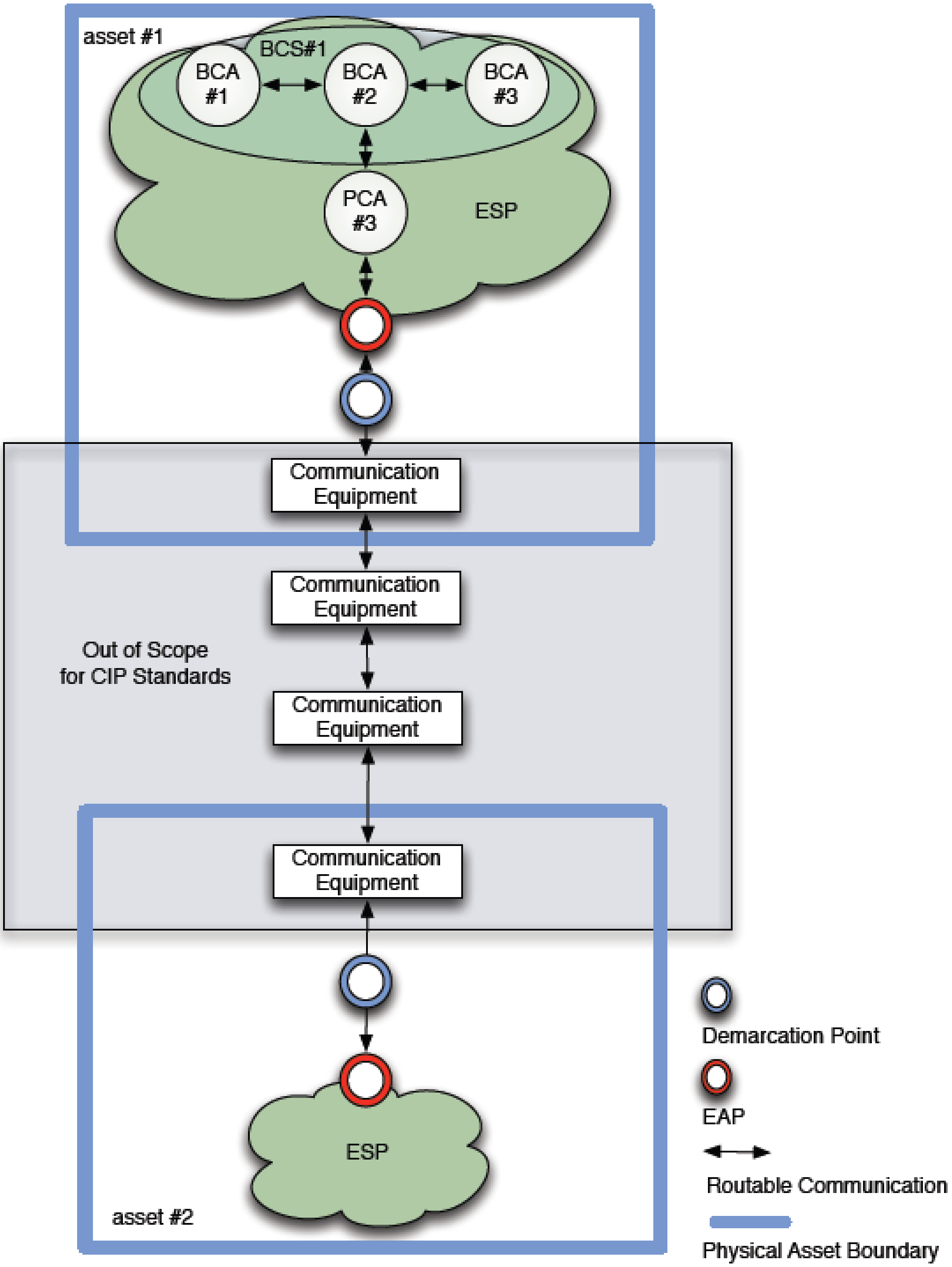

asset #1
BCS#1
BCA #1
BCA #2
BCA #3
PCA #3
ESP
Communication Equipment
Communication Equipment
Out of Scope for CIP Standards
Communication Equipment
Communication Equipment
ESP
asset #2
Demarcation Point
EAP
Routable Communication
Physical Asset Boundary

Figure 1

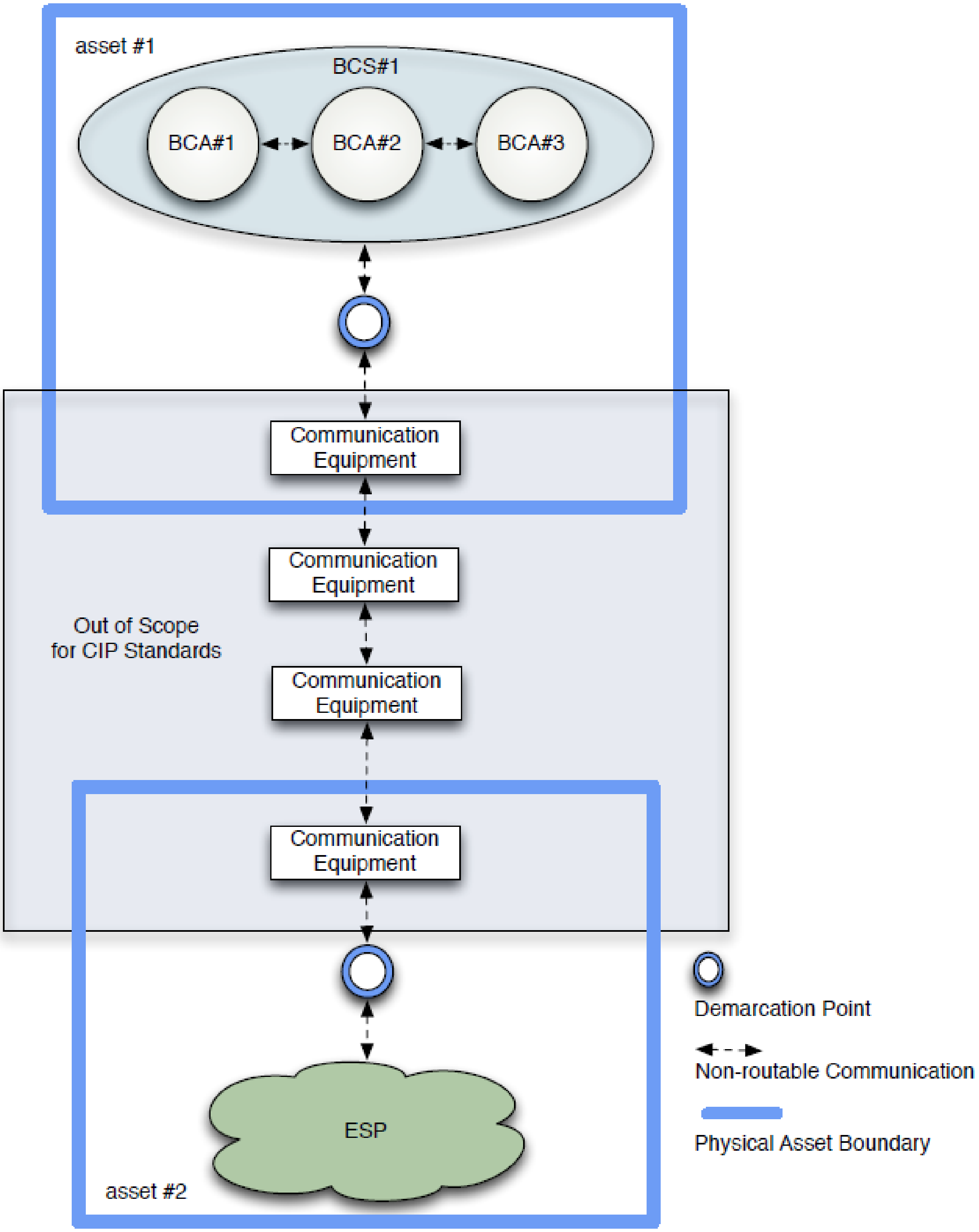

asset #1
BCS#1
BCA#1
BCA#2
BCA#3
Communication Equipment
Communication Equipment
Out of Scope for CIP Standards
Communication Equipment
Communication Equipment
ESP
asset #2
Demarcation Point
Non-routable Communication
Physical Asset Boundary

Figure 2

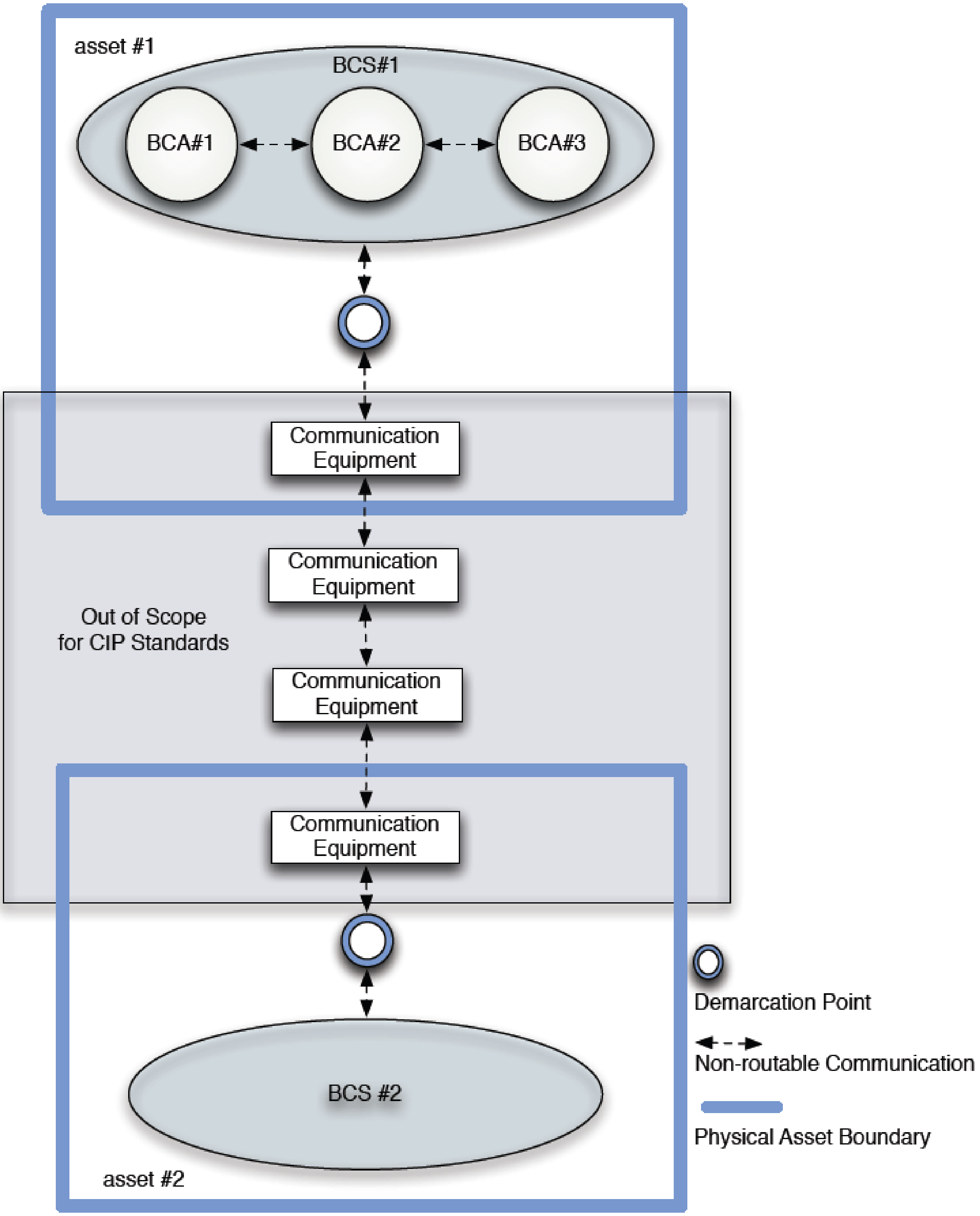

asset #1
BCS#1
BCA#1
BCA#2
BCA#3
Communication Equipment
Communication Equipment
Out of Scope for CIP Standards
Communication Equipment
Communication Equipment
BCS #2
asset #2
Demarcation Point
Non-routable Communication
Physical Asset Boundary

Figure 3

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

Industry Comments Draft Posted August 18, 2015
September 22, 2015

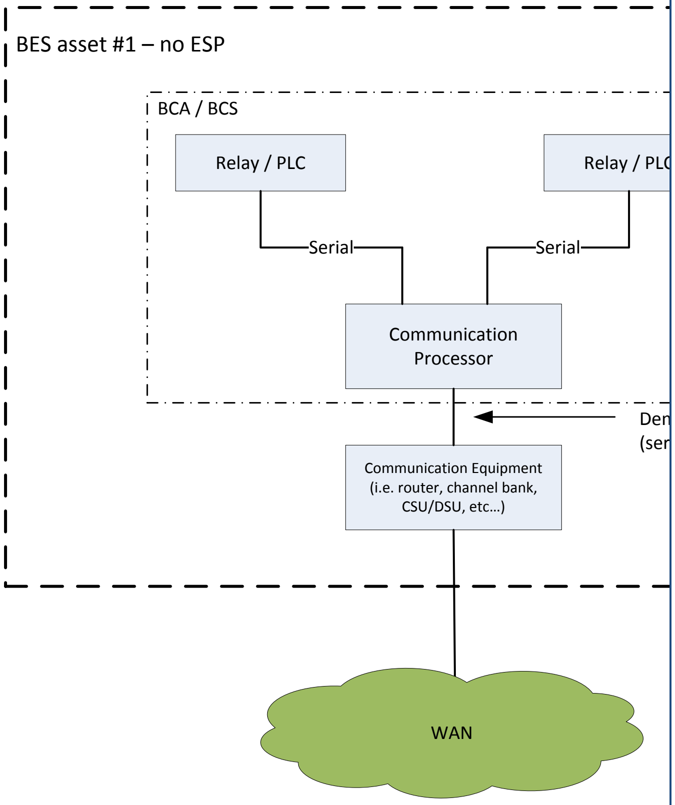
Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets

Organization	Comment	NERC Response	#
General Comments			
EnergySec	Although EnergySec is sympathetic to the apparent objective of this Lessons Learned, we believe there are significant issues with the approach presented. Additionally, the suggestions made by this Lessons Learned address interpretive issues and issues that are not explicitly addressed in the standard. We do not believe that these issues are appropriate for a Lessons Learned, or the recently proposed “Application Guidance” approach. We suggest that these topics be addressed via a formal Request For Interpretation and/or further standards development effort. Despite our concerns about the document as a whole, we offer the following comments and suggestions. General Comments: The model diagrams are referenced at specific sections of the document. It would make the document clearer and easier to read if the diagrams directly followed the sections they are related to. Other guidance documents released by the Version 5 Transition Advisory Group have included a section that includes relevant definitions from the the NERC Glossary of Terms. While it is true that a reader could look those up from the NERC Glossary while they are reading the Lesson Learned documents, we believe that having them included in the Lesson Learned document		1

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets			
Organization	**Comment**	**NERC Response**	**#**
	makes reading and understanding the document easier. In particular, since the definitions of BES Cyber Asset, Protected Cyber Asset, and Electronic Security Perimeter are central to the topics covered in this document, we believe it to be beneficial to include the official definitions of those terms. The document speaks often about choosing a "demarcation point" which is used to determine which networking devices are in scope and which networking devices are out of scope. There is minimal discussion, however, on how that demarcation point should be chosen. Since choosing the wrong demarcation point would lead to either increased costs associated with applying the CIP standards to devices for which it is not necessary, or a possible violation, additional guidance on choosing this demarcation point is necessary. We offer a suggestion on this topic later in these comments.		
MidAmerican Energy Company	MidAmerican Energy Company supports the Edison Electric Institute comments on the lessons learned posted for comment August 19, 2015, with comments due September 18, 2015: • Communications and Networking Cyber Assets Lesson Learned		2
Specific Comments			
Burns & McDonnell	After careful reading it became clear that Entities having BES assets (facilities) with no ESP will need to determine the Cyber Assets providing "local" communications for the BES asset and those Cyber Assets used to provide "external" communications into and out of the BES asset to determine those Cyber Assets in-scope for the CIP standards. From the text and provided figures (2 and 3) it appears the interconnection between the "local" Cyber Assets and those Cyber Assets providing the "external" communications be identified as a "demarcation		3

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets			
Organization	**Comment**	**NERC Response**	**#**
	point" for the purposes of determining the Cyber Assets in-scope of the CIP standards (i.e. BCA/BCS) at the BES asset. This is covered in the section titled "Communication and Networking Devices between an ESP and No ESP" on page 3 with the sentence which states: "The participant established a demarcation point that was between the BES Cyber System and the communication equipment used for external communications." This sentence is used with Figure 2 on page 6 of the LL which displays the "demarcation point" as being a circle with a blue colored edge. It appears the "demarcation point" based on Figure 2 (and Figure 3) can be either a device or cable between the BCS's and the Communication Equipment, or ESP (depending on what part of the figure you are looking at). Burns & McDonnell feels it would benefit the industry to verify that the "demarcation point" can be either a device or cabling between devices. Below is an example figure where the cabling is designated as the "demarcation point":		

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets

Organization	Comment	NERC Response	#
	 BES asset #1 – no ESP BCA / BCS Relay / PLC Relay / PLC Serial Serial Communication Processor Den (ser Communication Equipment (i.e. router, channel bank, CSU/DSU, etc…) WAN If the designation of the "demarcation point" cannot be either a device or cable between devices, we recommend the provide diagrams and text in the LL be updated to make this clear.		
ACES	ACES agrees that any cyber device located inside an ESP should be considered a PCA, especially when it does not meet the definition of a BES Cyber Asset. The last statement, "The basis for exclusion is the unavailability, degradation or misuse of the external communications" does not adversely impact the local		4

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets			
Organization	**Comment**	**NERC Response**	**#**
	functioning of the BES Cyber System. It may be countered that loss of external communication prevents the remote control or data acquisition for the Facility, and while true, the reliability impact for remote control or data acquisition is not associated to the high or medium impact BES Cyber System. This Lesson Learn might need to be revised due to the FERC Directive regarding communications between control centers and data protection. We are concerned that this issue will not consistently be audited across Regions, as auditors do not have clear guidance networking asset exclusions that sit outside the ESP.		
EnergySec	Under "Purpose": "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." The requirements for asset identification are well-established in CIP-002. The existence or absence of an ESP does not modify the obligation to determine which assets are in-scope for CIP. Furthermore, the asset identification requirements occur prior to the identification of ESPs. The intended meaning of the quoted sentence may differ from what was written and should therefore be restated. Under "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." This statement is misleading. Under version 3, all in-scope assets were required to reside within a defined ESP. It therefore follows that assets outside of an ESP are out of scope. However, they are not out of scope due to their location relative to the ESP, rather, it is the opposite, they are outside the ESP because they are out		5

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets			
Organization	**Comment**	**NERC Response**	**#**
	of scope. The exemption for communication devices between discrete ESPs is therefore superfluous under version 3 of the standards. "The same exemption is included in Version 5 of the CIP Standards." EnergySec believes that this exemption remains superfluous under version 5 since the identification of BES Cyber Assets (BCA) occurs prior to the identification of ESPs. The existence or absence of an ESP is not relevant to the determination of BCA status. Reliability Standard CIP-005-5 Attachment 1 requires Responsible Entities to classify BES Cyber Assets based on their impacts to the reliability tasks performed at assets such as Control Centers, generation facilities, and transmission facilities. This should refer to Reliability Standard CIP-002-5 Attachment 1. 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. We agree with this statement since, as previously stated, we do not believe that the existence or absence of an ESP is relevant to the determination of BCA status. However, the emphasis on exclusion indicates a potentially undue bias towards eliminating devices from scope. We understand that the overriding premise of this Lessons Learned is to exclude certain communications devices used to support wide-area communications. While we are sympathetic to this objective, we believe the approach taken to accomplish it is in error. As an alternative, we point out that CIP-002 requires that BES Cyber Systems be identified only for asset types specified in R1 (subsection i. – vi.). This allows for the exclusion of communication devices outside of core BES facilities, including 3rd party facilities owned by telecommunication providers.		

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets

Organization	Comment	NERC Response	#
	Under “Network Devices Classified as BES Cyber Assets”: EnergySec appreciates and supports the approach described in this section of determining BCA status based on the impact of a device. This approach is consistent with the requirements of CIP-002 and the definition of BES Cyber Asset. “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.” Although we generally agree with this approach, we point out that the question is not whether the loss, degradation or misuse of the device would have an impact on the reliability tasks performed at the asset, but rather, whether the loss, degradation, or misuse of the device would have an adverse impact on a BES asset (or more specifically, Facilities, systems, or equipment). Suggested edit: “In contrast, the communication and networking devices that were only being used for external communications were not classified as BES Cyber Assets when their loss, degradation, or misuse would not cause an adverse impact on an asset.” This wording is consistent with the definition of BES Cyber Asset. Under “Communication and Networking devices between defined ESP’s”: The communication equipment that is out of scope is the equipment used for establishing external communications at any location. There are likely to be multiple devices used as communication equipment between the BCS, as demonstrated by the multiple boxes labeled “Communication Equipment” in Figure 2. The use of the phrase “establishing external communications” introduces some ambiguity into the document, as it is		

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets			
Organization	**Comment**	**NERC Response**	**#**
	unclear if it is referring to merely the "first hop" of communications, which deals with establishing external communications from inside the ESP to outside the ESP, or if it refers to all the steps along the communication path. Under "Network Devices and Communication Equipment Out of Scope": The basis for exclusion is the unavailability, degradation or misuse of the external communications does not adversely impact the local functioning of the BES Cyber System. Again, the determination is not whether the lack of availability, degradation, or misuse of a Cyber Asset would adversely impact the local functioning of a BCS. The question that must be answered in determining whether a Cyber Asset is a BES Cyber Asset is whether the unavailability, degradation, or misuse would adversely impact a BES asset. While the answer to both questions is often the same, it may not always be, and it is important for guidance documents to be accurate in their language and consistent with the definition of BES Cyber Asset. "The basis for exclusion is the unavailability, degredation or misuse of the external communications does not adversely impact the local functioning of the BES Cyber System. It may be countered that loss of external communication prevents the remote control or data acquisition for the Facility, and while true, the reliability impact for remote control or data acquisition is not associated to the high or medium impact BES Cyber System." It is not clear what the basis for this statement is. If the lack of remote control or lack of data acquisition would adversely impact the operation of a BES asset, then that loss would be an argument for the Cyber Asset to be declared a BES Cyber Asset. It would be necessary to look at each situation and determine, in that situation		

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets

Organization	Comment	NERC Response	#
	for that entity, whether the impact would be adverse under the BCA definition.		
EEI	We do not have substantial comments for this lesson learned, but offer the following minor edits to help improve the document: 1. In the first sentence in the Purpose section there is an extra space between "approaches" and the period that ends the sentence. 2. Second paragraph in the Background section on page 1, we recommend changing CIP-005-5 to CIP-002-5.1. 3. CIP-002-5.1 does not require classification of low impact BES Cyber Assets; it requires the identification of high and medium impact Cyber Systems and assets that contain a low impact BES Cyber System. We recommend editing the first sentence in the second paragraph in the Background section on page 1 to be consistent with the requirement. For example, the sentence could be changed to: "Reliability Standard CIP-002-5.1 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." Alternatively, since this lesson learned is focused on high and medium BES Cyber Assets: "Reliability Standard CIP-002-5.1 requires Responsible Entities to identify high and medium impact BES Cyber Assets based on their impacts to the reliability tasks performed at assets such as Control Centers, generation facilities, and transmission facilities." 4. The first sentence on page 2 refers only to medium impact BES Cyber Systems, but should also include high impact BES Cyber Systems. We recommend adding "high and" before "medium impact."		6

Comments Received – CIP-002-5.1: Communications and Networking Cyber Assets

Organization	Comment	NERC Response	#
	5. Network devices can also be identified as BCA. We recommend adding “identified as BCA” before “(ii) identified as PCA.” 6. On page 4, under the Network Devices and Communication Equipment Out of Scope section, the first sentence of the second paragraph uses “degredation” should be changed to “degradation.”		
Manitoba Hydro	Manitoba Hydro has the following comments on communications and networking cyber assets LL: 1. Page 1 “CIP-005-5 Attachment 1” should be CIP-002-5.1 Attachment 1 2. Can you give some typical examples at control centre and substation on what are demarcation points for non-routable connectivity on Figure 2 and Figure 3? Does a demarcation point have to be a cyber asset, or can it consist of either: a. a port on a cyber asset, or b. a specific point on cabling or other nonprogrammable communication components?		7