NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
CIP Version 5 Transition Program
CIP-002-5.1 R1: Grouping BES Cyber Assets

Version: September 8, 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, modify the requirements in any existing reliability standards, or provide an official interpretation. 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 describe useful methods to group BES Cyber Assets (BCA) into BES Cyber Systems (BCS).

Background

The CIP Version 5 standards introduces a new concept not included in Version 3—a BES Cyber System, which consists of "one or more BES Cyber Assets (BCA) logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."

Guidance

Registered entities may choose to create different groupings of BES Cyber Assets to comply with individual CIP Version 5 standards. Entities are provided flexibility in how they group their BES Cyber Assets. However, it is recommended that each entity should document their processes for grouping their BES Cyber Assets to improve transparency during compliance monitoring. The following sections provide examples of how different participants in NERC CIP version 5 implementation study grouped their BES Cyber Assets into BES Cyber Systems.

Groupings Based on Function

Certain implementation study participants grouped their BES Cyber Assets by function. In other words, the entity grouped BES Cyber Assets into BES Cyber Systems based primarily on which BES Cyber Assets perform a common function. For example, an Energy Management System (EMS) BES Cyber System may consist of a number of human–machine interface workstations, communications servers, processing servers, database servers, and peripheral devices such as time-synchronizing clocks or printers.

All the EMS servers at a Control Center and the associated backup Control Center could be grouped together as they are categorized at the same impact level. Alternatively, entities can group Microsoft Cyber Assets, Linux Cyber Assets,

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

and other Cyber Assets (e.g., network or disk servers) according to the software patching requirements (as the patch sources may be different and released on different release cycles). This grouping methodology allows entities to prepare their processes and demonstrate compliance of like systems. Figure 1 illustrates how an entity may choose to group BCA based on function.

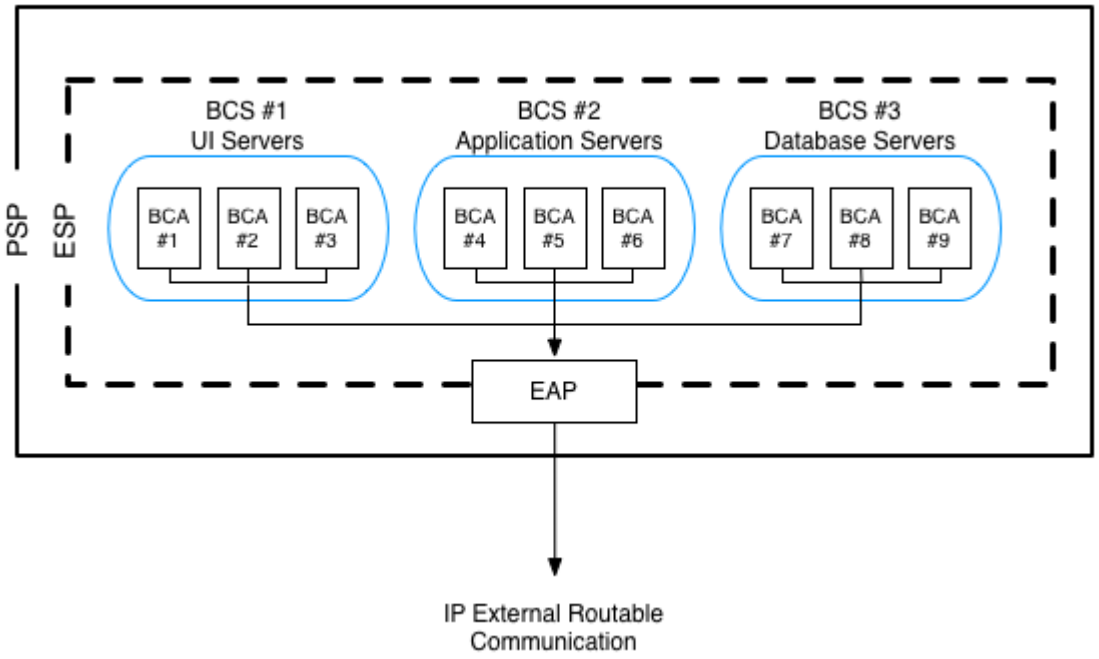

Figure 1: Functional Grouping

Groupings Based on Common Local Area Network

Other implementation study participants used a BES Cyber System grouping based on whether individual BES Cyber Assets are on a common local area network and can communicate with each other via a routable protocol. For example, a transmission protection system identified as a BES Cyber System could include all of the protective relay BES Cyber Assets at a specific transmission substation, especially if various protective relays communicate with each other over a local area network for protection coordination. While initially it may seem prudent to create separate BES Cyber Systems for each protection zone or for those protecting a single Facility at a given station or substation, there may be communications between different protection zones, either to provide additional zones of protection or backup within a specific zone. If the various protection systems identified as BES Cyber Systems need to meet the same CIP standard requirements, there may be no benefit in creating multiple separate BES Cyber Systems at a transmission station. However, if it is anticipated that (1) some BES Cyber Systems will be at different impact ratings (e.g., medium or low), (2) there is limited or no communications between the BES Cyber Systems at different impact levels, and (3) they are not on the same local area network, then having multiple BES Cyber Systems may be a preferable approach. See Figure 2 below.

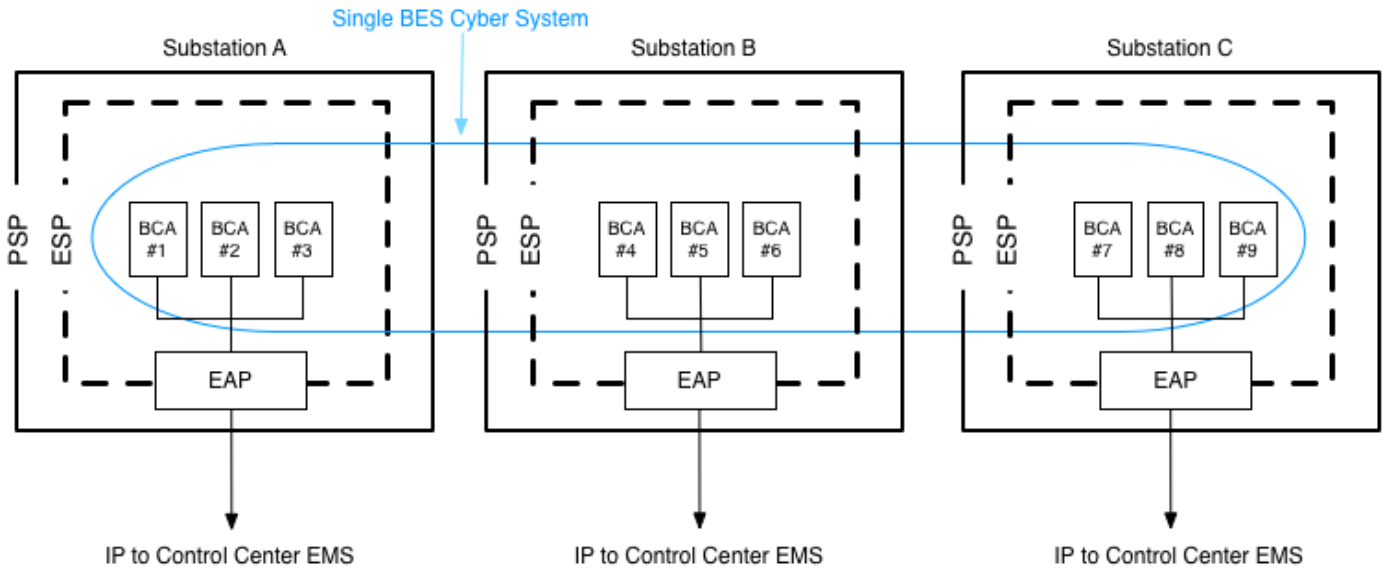

Figure 2: Grouping across Substations

Additional Examples

One implementation study participant identified several BES Cyber Assets at a medium impact substation and elected to group them into BES Cyber Systems based on both function and location as described above. The entity has grouped the remote terminal unit (RTU) equipment together as one BES Cyber System and the Protection Systems equipment together as another BES Cyber System. The BES Cyber Assets in each BES Cyber System work together to provide the same BES reliability operating services and the loss of one asset in the system impacts the functions of the system in a similar manner. See Figure 3 below.

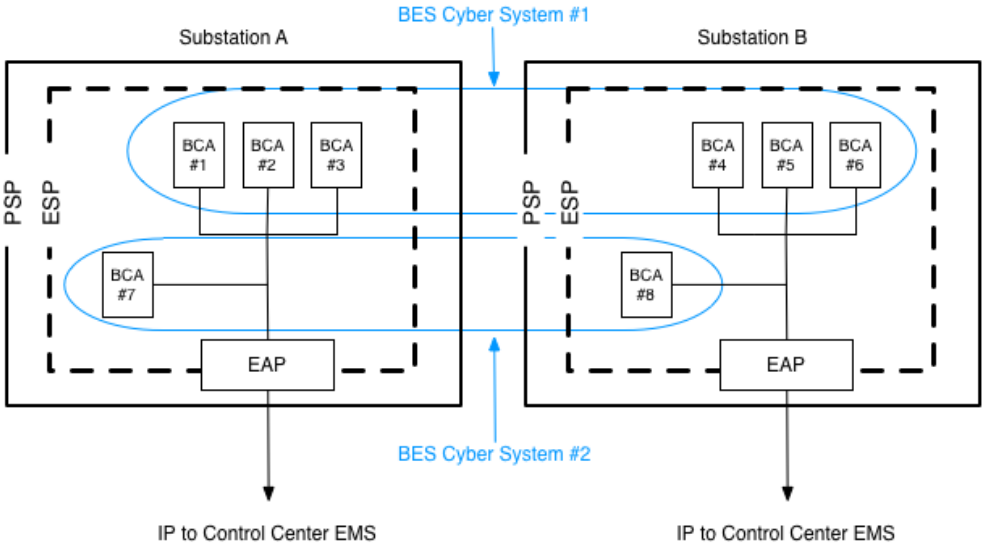

Figure 3: Grouping by Function and Location

Alternatively, entities may choose to group all of the BES Cyber Assets at a particluar medium impact substation into a BES Cyber System, i.e. grouping by physical location, as in figure 4 below.

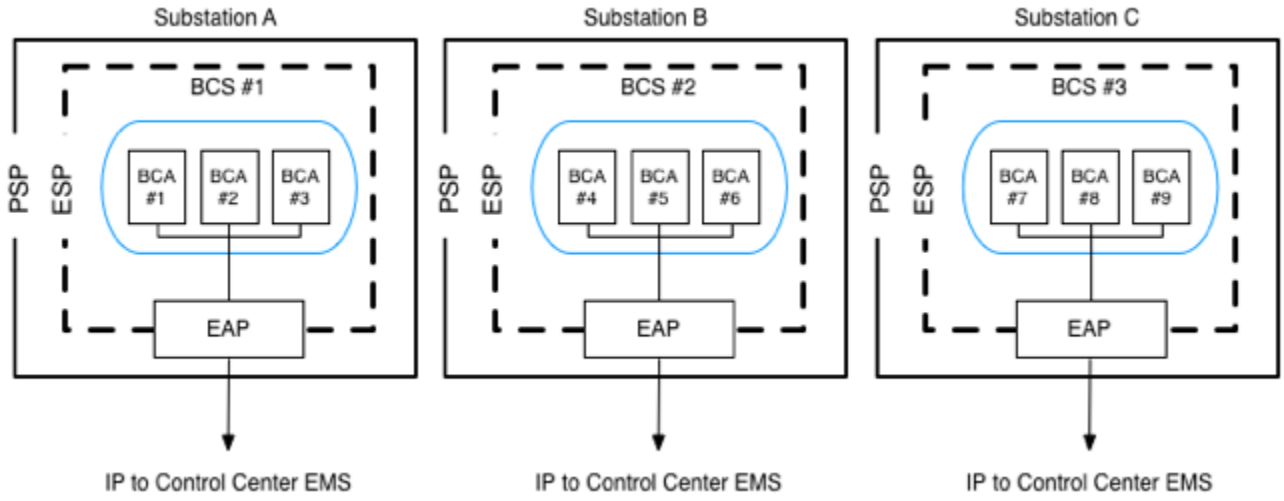

Figure 4: Grouping by Location

Notwithstanding the previous examples, there are many options for grouping BES Cyber Assets into a BES Cyber System. An entity may choose to group BES Cyber Assets into individual BES Cyber Systems based on connectivity type. For example in Figure 5, at a medium impact substation, all Protection System BES Cyber Assets with External

Routable Connectivity would be one BES Cyber System, all Protection System BES Cyber Assets without External Routable Connectivity would be another BES Cyber System.

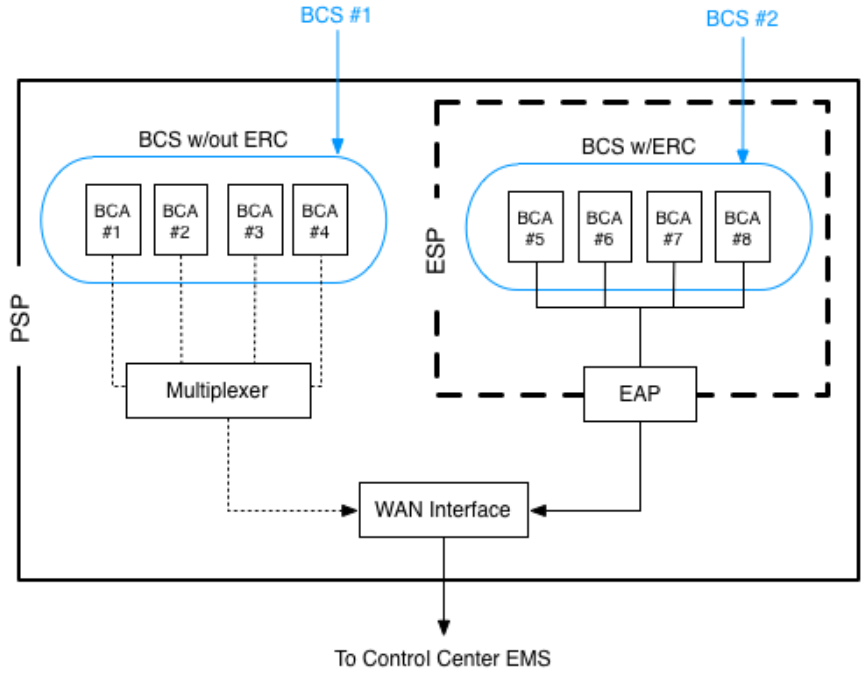

Figure 5: Grouping by Connectivity

Alternately, the entity could group all BES Cyber Assets with External Routable Connectivity (e.g., RTU equipment, protection systems) at the substation into one BES Cyber System. However the BES Cyber System is defined, it must meet the CIP v5 standard requirements at the system level for all of its component BES Cyber Assets. A BES Cyber Systems can cross Physical Security Perimeters (PSP), Electronic Security Perimeters (ESP), and Facility geographic boundaries; they can encompass many Physical Security Perimeters, Electronic Security Perimeters and Facilities.

Documenting BES Cyber Systems

The inventory list created through the development of CIP-002-5.1, Requirement R1 should indicate the identified BES Cyber System groupings. To demonstrate compliance, one approach is to create a name for each individual BES Cyber System for reference when applying the remainder of the requirements of the CIP Version 5 standards. As provided in the example below, a reason (or reason code) to document the rationale for the grouping would also be beneficial when presenting your evidence for audit. Though not required by the CIP-002-5.1, one way to document this approach could be in a sortable spreadsheet, as shown below:

No.	Facility Name	Equipment Description	Device ID	Responsible Work Group	Function	Cyber Asset Classification (BCS)	BES Reliability Operating Service (BROS)	If not a BCA - List the reason why	PSP	ESP

Grouping BES Cyber Assets Considerations

- Groupings may assist an entity in placing controls around devices that would otherwise not be able to apply a particular control, e.g. CIP-007-6 R4.1, logging at the systems or asset level.

- BCS groupings do not influence or change other CIP concepts, such as ESP, PSP, impact rating, watermarking, ERC, Facilities or brightline when grouping BCAs of the same impact rating.

- While it is possible to place a single BCA in more than one BCS, doing so creates complexity in documenting compliance for the entity and verification of compliance by the regional entity. Entities should exercise caution if planning to group in this manner.

- Entities may choose to consider carefully documenting the strategies for grouping a BCA into a BCS, e.g. based on LAN, function, geolocation, etc, as a matter of good practice, and entities should be prepared to provide the grouping upon receiving the 90 day audit notification. The Request For Information (RFI) may be customized by the region based on an entities grouping.

- Care should be taken when grouping across impact ratings. When there are multiple impact rated BCAs inside a single BCS, all assets must be protected to the highest impact rated BCA contained within the BCS.

- Entities may choose to consider documenting which controls are being applied at the system level and which are being applied at the asset level.