NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
CIP Version 5 Transition Program

CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems

Version: January 29, 2015

Authorized by the Standards Committee for posting as a supporting reference pursuant to section 11 of the Standard Processes Manual on February 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 describe the options used by Study Participants for identifying and categorizing, consistent with Reliability Standard CIP-002-5.1 Requirement R1 and Attachment 1, criteria 2.1, their BES Cyber Systems located at 1500 MW generation resources[1]. In short, entities must: (1) categorize the shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection at such a generating resource as medium impact BES Cyber Systems; and (2) categorize all other BES Cyber Systems at such generating resource as low impact BES Cyber Systems[2] and the generation resource as an asset containing low impact BES Cyber Systems. Segmentation of the generating units and their associated BES Cyber Systems at the generation resource can be used to show that BES Cyber Systems for each segmented unit, or group of units, does not meet the medium impact criteria 2.1 of Attachment 1 to Reliability Standard CIP-002-5.1.

This Lesson Learned also discusses the type of evidence that a Responsible Entity could provide to demonstrate that it appropriately identified and categorized their BES Cyber Systems at 1500 MW generation resources, in particular, whether the generation units and associated BES Cyber Systems have been sufficiently segmented such that a shared BES Cyber System does not meet the medium impact

[1] For the purposes of this document, the term "1500 MW generation resource" is defined as "commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection."

[2] A discrete list of low impact BES Cyber Systems is not required per CIP-002-5.1 R1.3

rating criteria 2.1 in Attachment 1 of Reliability Standard CIP-002-5.1 and is correctly categorized as a low impact BES Cyber System.

Lesson Learned

The categorization of shared BES Cyber Systems as medium impact at a 1500 MW generation resource depends on the configuration of the generation resource, namely the configuration and segmentation of the generating units and associated BES Cyber Systems. If, for instance, the generation units and BES Cyber Systems are connected in a manner that could adversely impact 1500 MW or more if any shared BES Cyber Systems were unavailable, degraded, or misused, then those shared BES Cyber Systems (i.e., those that can, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection) must be categorized as medium impact BES Cyber systems. If, on the other hand, the generating units and BES Cyber Systems are sufficiently segmented such that unavailability, degradation, or misuse of shared BES Cyber Systems would not result in the loss of 1500 MW within 15 minutes, then those BES Cyber Systems need not be categorized as medium impact and the generation resource would be categorized as an "asset containing low impact BES Cyber Systems." [3] In short, Responsible entities may thus choose to protect their BES Cyber Systems at 1500 MW generation resources in one of the following ways:

A. **Protect the BES Cyber Systems categorized as Medium Impact at a Single Plant Location.** Responsible Entities may choose to protect the medium impact BES Cyber Systems at a 1500 MW generation resource by applying all the CIP standard (CIP-002-5.1 through CIP-011-1) requirements that are applicable to medium impact BES Cyber Systems.

B. **Segment the Generating Units and Their Associated Shared BES Cyber Systems.** Responsible Entities may choose to segment generating units at a 1500 MW generation resource and their associated BES Cyber Systems such that each segmented unit, or group of units, and their associated BES Cyber Systems do not meet the 1500 MW criteria described in CIP-002-5.1, Attachment 1, Criterion 2.1. Segmenting generating units and their associated BES Cyber Systems can reduce risks to the reliable operation of the BES. In this case, entities must protect each of the generating units or group of units as assets containing low impact BES Cyber Systems.

   If a Responsible Entity adopts the segmentation approach, consistent with criterion 2.1, entities must provide evidence that shared BES Cyber Systems associated with any group of generating units at 1500 MW generation resources are segmented effectively such that there are no shared BES Cyber Systems that could result in the loss of 1500 MW or more of generation within 15

[3] Under CIP-002-5 Requirement R1, generating plant sites that have net Real Power capability of less than 1500 MW would be identified and categorized as "assets containing low impact BES Cyber Systems," provided such plants do not meet any other high or medium impact criteria in CIP-002-5, Attachment 1.

minutes.[4] Identifying shared BES Cyber Systems involves detailed analysis that considers shared generating plant operational processes (e.g., air, water, steam, environmental, and fuel handling processes) and electronic connectivity. Figure 1 below provides an example flow chart used by one Responsible Entity to categorize BES Cyber Assets at a 1500 MW generation resource.

This evidence could include analyses that demonstrate effective segmentation of, for example:

- BES Cyber Systems protected by the segmented unit network(s).
- Generating plant operational processes shared by multiple generating units or group of units, and analysis that unavailability, degradation, or misuse of the shared BES Cyber Systems that operate those operational processes would not impact 1500 MW or more within 15 minutes.
- BES Cyber Systems shared by multiple generating units or group of units, and analysis that unavailability, degradation, or misuse of the BES Cyber Systems could not impact 1500 MW or more within 15 minutes.
- Access restrictions on network interfaces between each generating unit or group of units and external networks (e.g., firewall rules).

Background Information

Relevant CIP Version 5 Standard Requirements

CIP-002-5 Attachment 1, Section 2.1 provides that BES Cyber Systems at the following generation resources meet the medium impact rating:

> Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Relevant Definitions in the NERC Glossary of Terms:

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

[4] Shared BES Cyber Systems are typically introduced through common connectivity between systems on multiple units or common generating plant operational processes that can affect more than one unit.

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.

Cyber Assets – Programmable electronic devices, including the hardware, software, and data in those devices.

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

Physical Security Perimeter (PSP) – They physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Relevant CIP Version 5 Standard Guidelines and Technical Basis

The Guidelines and Technical Basis section of Reliability Standard CIP-002-5 provides the intent of the standard drafting team regarding the Medium Impact Rating for generation resources as follows:

> "By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected."

Figure 1: Sample BES Categorization Flow Charts for 1500 MW Generation Resources

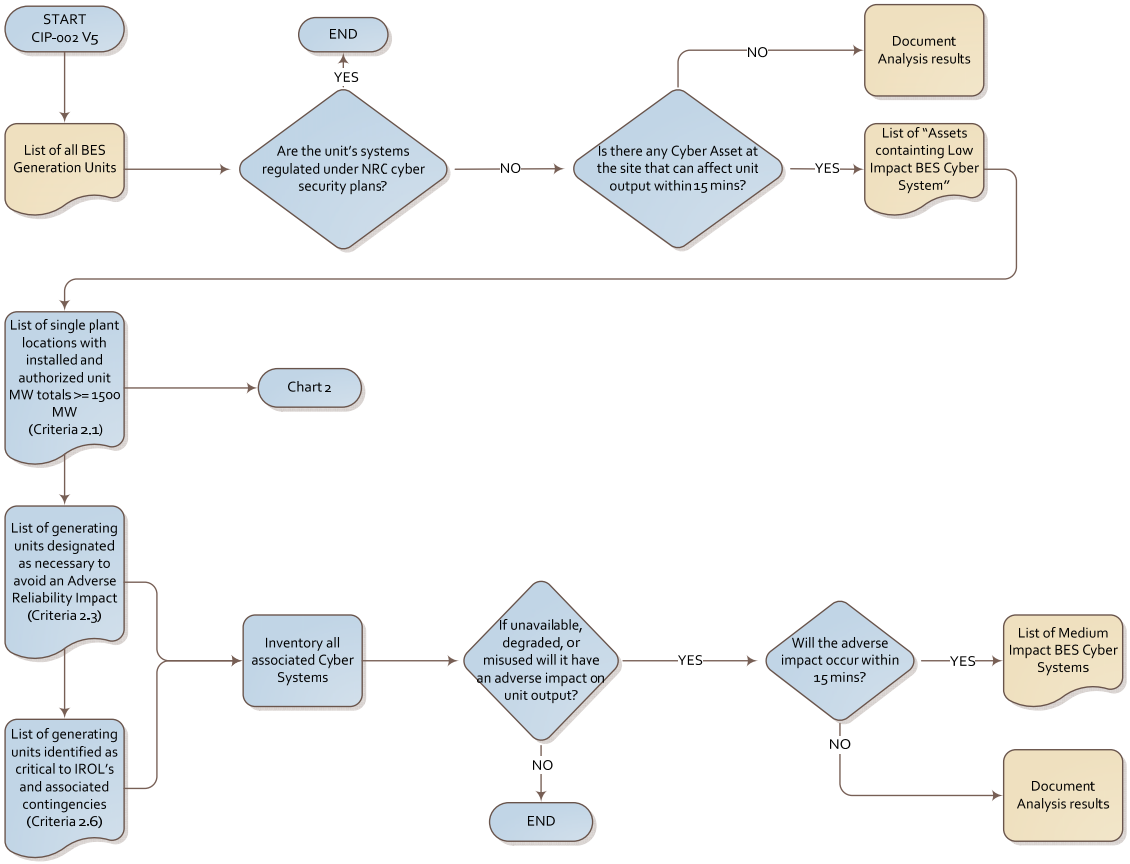

Chart 1

CIP-002 Version 5 - Determination of Medium/Low Impact BES Cyber Systems For Generation Resources

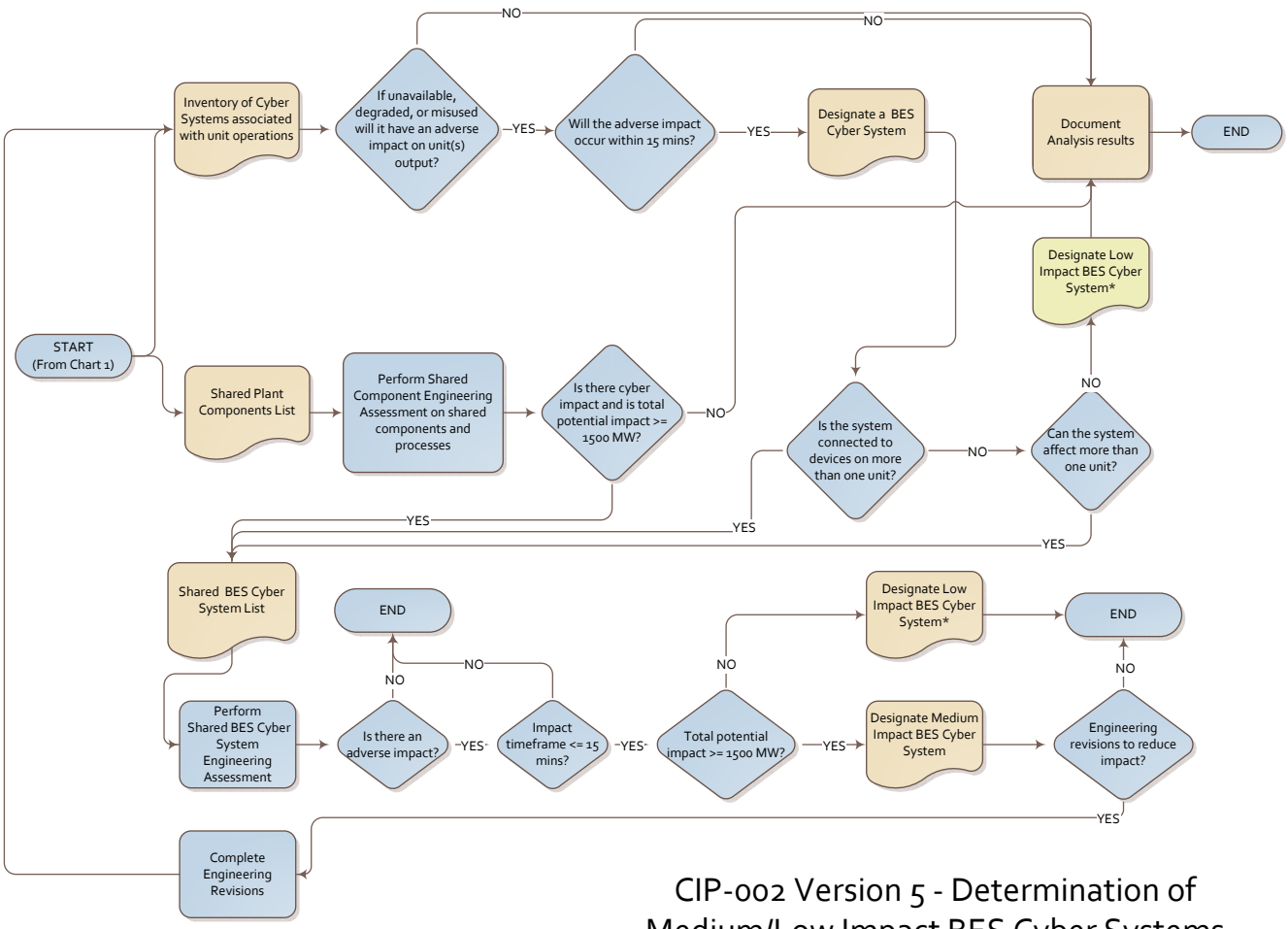

Chart 2

*Note: CIP-002-5.1 does not require inventories of low impact BES Cyber Systems.

CIP-002 Version 5 - Determination of Medium/Low Impact BES Cyber Systems For 1500 MW Generation Resources