STANDARDS COMMITTEE
MIDWEST RELIABILITY ORGANIZATION

STANDARD APPLICATION GUIDE

CIP-002-5.1

Report Date: January 8, 2015

Revised: February 18, 2015
(*Revisions listed on page 69)*

Authored by

Ron Bender, *Nebraska Public Power District*
Jesse Consolatti, *Alliant Energy*
Sharon Koller, *American Transmission Company*
Marie Knox, *MISO*
Marc Child, *Great River Energy*
Bruce MacKenzie, *Saskatchewan Power*
Charles Lawrence, *American Transmission Company*

The MRO Subject Matter Expert Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

Disclaimer

The Midwest Reliability Organization (MRO) Standards Committee (SC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging Reliability Standards. Any materials, including presentations, were developed through the MRO SC by Subject Matter Experts (SMEs) from member organizations within the MRO Region.

In 2013, SMEs in the field of Cyber Security were brought together to prepare a guide for complying with NERC Reliability Standard CIP-002-5.1 (Cyber Security - BES Cyber System Categorization). Participants include representatives from Balancing Authorities (BAs), Reliability Coordinators (RCs), Generator Operators (GOPs), and Transmission Operators (TOPs).

CIP-002-5.1 Application Guide – Development Team Subject Matter Experts

Sharon Koller, Chair
Charles Lawrence, Alternate
American Transmission Company

Marc Child, Vice Chair
Great River Energy

Ron Bender
Nebraska Public Power District

Marie Knox
MISO

Jesse Consolatti
Alliant Energy

Bruce MacKenzie
Saskatchewan Power

The materials have been assessed by MRO staff and provide reasonable application guidance for the standard(s) addressed. Ultimately, demonstrating compliance depends on a number of factors including the precise language of the standard, the specific facts and circumstances, and quality of evidence.

Acknowledgement

This publication was developed by a team of SMEs from MRO member organizations within the MRO footprint. The development of SME teams is an ongoing effort to produce unified application guides for MRO and its Registered Entities.

The CIP-002-5.1 SME Team Chair, Sharon Koller (*American Transmission Company*), wishes to acknowledge and thank those who dedicated efforts and contributed significantly to this publication. The MRO, MRO SC and their organizational affiliations include:

Midwest Reliability Organization

James Burley, Vice President
Risk Assessment and Mitigation and Standards

Russ Mountjoy, Manager
Standards, Registration, and Certification

Jennifer Matz, Administrator
Risk Assessment and Mitigation and Standards

MRO Standards Committee

David Rudolph, Chair
Basin Electric Power Cooperative

Joe Knight
Great River Energy

Jason Burki
Alliant Energy

Robert Thompson, Vice Chair
Xcel Energy

George Brown
Acciona Energy

Wayne Guttormson
Saskatchewan Power

Michael Moltane
ITC Holdings

Todd Komplin
WPPI Energy

Andrew Pusztai
American Transmission Company

Mark Buckholz
Western Area Power Administration

TABLE OF CONTENTS

INTRODUCTION 5
OVERVIEW 9
METHODOLOGY 10
General CIP Program Recommendations 10
Methodology / Approach Rationale: 13
Recommended Approach (Approach 1): 16
BES Cyber Systems – Additional Guidance 27
Evaluating CIP-002-5.1, Requirement 1 31
Evaluating CIP-002-5.1, Requirement R1.1 35
Evaluating CIP-002-5.1, Requirement R1.2 39
Evaluating CIP-002-5.1, Requirement R1.3 57
Evaluating CIP-002-5.1, Requirement 2 62
MITIGATING RISK AND INTERNAL CONTROLS 64
APPENDIX A: REFERENCES 65
APPENDIX B: COMPANION DOCUMENTS 66
APPENDIX C: RECOMMENDED APPROACH 67
APPENDIX D: TOP-DOWN VARIATIONS 68

INTRODUCTION

NERC Reliability Standard CIP-002-5.1 (BES Cyber System Categorization) serves an important purpose by requiring functional entities to identify and categorize Bulk Electric System (BES) Cyber Systems and their associated BES Cyber Assets.

Purpose (CIP-002-5.1 Section 3):

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

Note 1: The use of undefined terms introduces risk that could lead to variances in interpretation as it relates to the identification of BES Cyber Systems and their relationship to impact-rated BES Facilities. In the context of Medium impact, CIP-002-5.1 Requirement R1.2 uses the term "at," and the Attachment 1, Section 2 Medium Impact Criteria utilizes the terms "associated with." Registered Entities could interpret that the Requirement language is to be used in conjunction with the Attachment 1 Impact Rating Criteria, and thereby conclude that the word "at" the end of R1.2 means "both." With this interpretation, a Registered Entity could further conclude that BES Cyber Assets/Systems must be both "at" and "associated with" the identified "BES Facility" to qualify as a Medium Impact-rated. When comparing this literal interpretation to the myriad variations of how BES Facilities and systems could be related, it stands to reason that a different conclusion is that BES Cyber Assets/Systems could exist at a geographic location not literally co-located at the BES asset containing the identified impact-rated BES Facility. As a result, entities are encouraged to employ Cyber Asset candidate identification methods that consider not only those Cyber Assets at the BES asset, but also those Cyber Assets that may be relevant to the BES Facility independent of physical location. One potential approach to achieve this level of rigor without literally inventorying and analyzing every single Cyber Asset not physically located within the BES asset may be to consult the configuration of Cyber Assets used to control electronic access to/from Cyber Assets at the BES asset. This approach is one that could identify geographically separated Cyber Assets that may qualify as BES Cyber Assets associated with the BES Facility. As one example, where a Medium BES Cyber Asset (MBCA) has External Routable Connectivity an entity could leverage the firewall rule set controlling access to/from that MBCA to identify those Cyber Assets that can remotely connect. Once those other Cyber Assets are identified, the entity could evaluate them to determine if they qualify as a BES Cyber Asset associated with the BES Facility. Supplementing a physical inventory of Cyber Assets at the BES asset with an approach like, but not limited to, this may provide a more comprehensive approach to this identification process as well as greater assurance that Cyber Assets associated with the BES Facility are identified and protected.

Note 2: This document is one of a body of work. Companion documents that support this application guide consist of Attachment 1 Criteria application workbooks, Version 3 to Version 5 transition guidance, example diagrams, and a sample standard operating procedure. A list of companion documents exists in Appendix B.

Applicability (CIP-002-5.1 Section 4):

4.1 ***Functional Entities:*** *For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.*

4.1.1 ***Balancing Authority***

4.1.2 ***Distribution Provider that owns*** *one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:*

4.1.2.1 *Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:*

4.1.2.1.1. *is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and*

4.1.2.1.2. *performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.*

4.1.2.2. *Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.*

4.1.2.3. *Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.*

4.1.2.4. *Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.*

4.1.3 ***Generator Operator***

4.1.4 ***Generator Owner***

4.1.5 ***Interchange Coordinator or Interchange Authority***

4.1.6 ***Reliability Coordinator***

4.1.7 ***Transmission Operator***

4.1.8 ***Transmission Owner***

4.2 *Facilities:* *For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.*

4.2.1. Distribution Provider*: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:*

4.2.1.1. *Each UFLS or UVLS System that:*

4.2.1.1.1. *is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and*

4.2.1.1.2. *performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.*

4.2.1.2. *Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.*

4.2.1.3. *Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.*

4.2.1.4. *Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.*

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers*: All BES Facilities.*

4.2.3. Exemptions: *The following are exempt from Standard CIP-002-5.1:*

4.2.3.1. *Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.*

4.2.3.2. *Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.*

4.2.3.3. *The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.*

4.2.3.4. *For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.*

Requirements:

R1. *Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning]*

- ***i.*** *Control Centers and backup Control Centers;*
- ***ii.*** *Transmission stations and substations;*
- ***iii.*** *Generation resources;*
- ***iv.*** *Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;*
- ***v.*** *Special Protection Systems that support the reliable operation of the Bulk Electric System; and*
- ***vi.*** *For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.*

1.1. *Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;*

1.2. *Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and*

1.3. *Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).*

R2. *The Responsible Entity shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 *Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and*

2.2 *Have its CIP Senior Manager, or delegate, approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.*

OVERVIEW

This Standard Application Guide (SAG) it meant to be read from cover to cover, like a book, or a reference guide.

This SAG focuses on the NERC Reliability Standard CIP-002-5.1 (Cyber Security – BES Cyber System Categorization). FERC has approved this standard, and subsequently FERC Order 791, which directed NERC to make adjustments to the approved standards. The authors are aware that this order will have an impact on the controls required for Low Impact; Communication Networks; Identify, Assess, and Correct (IAC) language; Transient Devices; and the BES Cyber Asset definition.

This SAG uses terms defined in the NERC Glossary of Terms. The CIP Subject Matter Expert (SME) Team was deliberate in the use of those terms and careful to capitalize the first letter of defined terms in an effort to prevent confusion or ambiguity. In some instances, the first letter of a term is also underlined to further emphasize the significance of the letter-case to the reader so it is interpreted in the correct context. Where the CIP SME Team introduced terms not defined by NERC, as necessary, inline definitions or narratives around the intent of those terms has been provided. As an example, there is a significant distinction between the terms Facility and facility, where the first is defined by NERC and prescriptive as to its meaning, and where the latter is undefined and this undefined term creeps into verbal discussions and some guidance references as a way of referring to buildings or assets like but not limited to stations, substations, plants, control centers, etc.

This Guide does not address Version 4 of the CIP Standards.

METHODOLOGY

This section contains suggested methodology to meet the requirements of the NERC CIP-002-5.1 Standard. These methods represent the intended best practices of members of the CIP-002-5.1 Subject Matter Expert (SME) Team.

General CIP Program Recommendations

While there are details within each requirement that require specific attention, some aspects of compliance are consistent throughout. Each recommendation in this section can be applied to both of the requirements. When developing the individual components of a compliance program, each of these recommendations should be revisited. Where any of these can be uniquely applied to an individual requirement, they will be mentioned again in that section.

Documentation: "If you didn't document it, you didn't do it." Many of the requirements speak directly to documenting a program or process. However, not all documents are created equal.

- Structure – Documents used for compliance should have components that assure inclusion of necessary information, change management, and references to other relevant documents. Remember your audience and choose a format that allows users and auditors to find information quickly and easily. Helpful components include: Owner/Approver, Definitions, Purpose (mapped to the CIP requirement addressed), Procedure, etc.
- Revision history –Revision history makes it possible to demonstrate that revisions are made in accordance with implementation deadlines, procedural change timeframes, annual reviews, etc. Keeping revision history will establish point-in-time compliance. It is also helpful to have a summary of what changed with each revision. Maintain revision history for the duration of the audit period.
- Roles and Responsibilities – Written procedures are a great way to assure that each individual knows his or her role in the process. Additionally, they help add clarity in identifying a SME to participate during an audit.
- Tip: Unless required by the Standards, use titles not names.

Evidence Considerations: Evidence is more than just documentation. Demonstrating compliance usually means "corroborating" evidence. In other words, compliance programs should be designed to produce an output of several auditable records for each requirement to demonstrate performance. A documented process is the first part of demonstrating compliance. Additional suggested critical and/or supporting evidence is included within this guidance document. For each requirement, a documented process and at least one other additional record should be available to demonstrate compliance.

The best types of evidence are consistent throughout the organization. For example, NERC CIP changes should require the same request form and follow the same processes, yielding exactly the same types of output. They should also provide reliable time/date stamps that are difficult to falsify. As an example, screen captures should include a visible time and date stamp within the capture.

Attestations provided for compliance activities are considered weaker evidence, which may need to be corroborated with stronger evidence. But where demonstration of a null list or the absence of an activity is necessary, an attestation may be the only record that can be provided in addition to the documented process; therefore, an attestation may be sufficient.

Reviews and/or Approvals: Another item expressly addressed throughout the CIP Standards is the requirement to conduct "reviews." Each documented process should be accompanied by how reviews are initiated, conducted, and tracked. Rigor and formality in this process will be rewarded. For each documented review and/or approval, the auditor should easily understand:

- Who was the reviewer and/or approver?
- What content was reviewed and/or approved?
- When was it reviewed and/or approved?
- What changes were made? If so, how were they communicated?

Definitions: Each requirement may contain words or phrases that are not entirely clear. Even "industry" terms can be applied differently in relation to a specific program or device. NERC has published, and continues to publish, documents that can be used to understand what is meant by the terms included in the Standards. These documents include, but are not limited to, NERC Glossary of Terms, Implementation Studies, Compliance Analysis Reports (CARs), Reliability Standard Audit Worksheets (RSAWs), interpretation documents, and other guidance documents. Even though these documents can provide assistance, it is the obligation of the Registered Entity to assure that the definition or interpretation in use is documented. It is reasonable to use definitions from trusted resources in the industry, but reliance on that definition should be supported in a documented part of the specific program to which it applies. In fact, even where using a definition provided by NERC, assure that definition is documented with the program for point-in-time understanding of the entity's implementation of CIP compliance.

References: There are many available guidance documents for writing emergency and operating plans, determining sound security practices, specifications for configuration of physical and electronic controls, industry standards, etc. Adhering to the guidance within those materials can aid in developing and maintaining compliance programs, as well as demonstrate rigor in researching available solutions. Maintain copies of source material to provide during audits, as this can help explain why specific elements were implemented.

Support: Within the organization, it is possible that disparate groups engage in the support of the assets within the scope of CIP compliance. Historically, segregated IT and business areas are sharing responsibilities and control in order to achieve compliance. Configurations required for compliance should be protected by strong change control processes and clear documentation outlining roles and responsibilities. Personnel who may only be peripherally involved in support of CIP assets, perimeters, and information should receive CIP training.

Correlation: Assure a broad understanding of all the NERC Reliability Standards (BAL, COM, CIP, EOP, FAC, INT, IRO, MOD, NUC, PER, PRC, TOP, TPL, VAR) when developing a CIP Compliance program. This understanding should include reporting obligations, definitions, and any cross-references. Ensure that documented processes are consistent throughout the Registered Entity's compliance programs.

Compliance Monitoring: When resources and time allow, internal and vendor audit resources should be considered for program definitions, targeted auditing, or full mock audits. The Registered Entity can rehearse interviewing, learn about its ability to respond to compliance monitoring scenarios or information requests, practice compiling evidence and documentation, and identify potential insufficiencies. It can also be helpful to check with neighboring entities for reliable vendors. Ongoing and transparent communications, and a pre-audit conference call or meeting with MRO audit staff is strongly encouraged by MRO to address questions and answers. As the enforcement model undergoes change from the historical and current "look back" audits and continues to align with the Reliability Assurance Initiative by focusing on an entity's inherent risk to the safe, secure, and reliable operation of the BES, entities are encouraged to stay apprised of updates to the Electric Reliability Organization (ERO) Compliance Monitoring and Enforcement Program (CMEP)[1] to maintain alignment with the current and compliance enforcement processes and tools, as well as the direction of emerging practices.

Collaboration: Within the constraints of information protection, Registered Entities can benefit from sharing program designs, interpretations, implementation tips, and audit experiences. Collaboration can result in innovative solutions to common problems, increased leverage when dealing with common vendors, as well as shared expertise and lessons learned. It is important to remember that individual audit experiences may vary, and information should be carefully weighed by each Registered Entity before action, even if that information is contained within this Guide.

Timing: Consider your compliance activities when scheduling major projects that may share personnel, technology, or other resources. Consider freezes on technology or process changes when preparing for a regional audit, schedule internal audit activities outside of self-certification windows, etc. Wherever possible, avoid competition and individual priorities will line up appropriately.

[1] See http://www.nerc.com/pa/comp/pages/reliability-assurance-initiative.aspx

Methodology / Approach Rationale:

In the development of this application guide the team considered two methods of applying CIP-002-5.1.

- (Approach 1) - Inventory and categorize facilities, then identify and classify Cyber Systems (facility-centric, or top-down)
- (Approach 2) - The second approach is the opposite, beginning with a BES Cyber Systems inventory, then a cross-reference to facilities (cyber systems centric, or bottom-up)

In comparing the two approaches (facilities-centric vs systems centric), each is comprised of two necessary methodological components that could be performed independently.

- A methodology to determine qualifying BES assets and BES Facilities
- A methodology to determine applicable BES Cyber Assets and Systems

Each methodological component is an exercise in candidate identification, criteria and attribute assessments, and filtering to derive an output. Once an output from each component is achieved, the final step is to associate the results for a combined output that defines the ultimate scope of CIP-002-5.1 BES assets and/or BES Cyber Systems requiring the applicable protective measures of CIP-003-5 – CIP-009-5 and CIP-010-1 – CIP-011-1.

Note: This methodology also reinforces the concept that two types of BES Cyber Systems at potentially different impact ratings could co-exist at one location.

Each methodological component begins with candidate inventories of assets and Cyber Assets. Through the process, those inventories are scoped to the purview of the CIP-002-5.1 applicability, requirements, impact rating criteria, and definitions within the NERC Glossary of Terms. Additionally, the authors of this Standards Application Guide have chosen to incorporate the optional concept of using the defined process of BES Reliability Operating Services (BROS) as documented in the Guidelines and Technical Basis section of CIP-002-5.1. Leveraging this NERC Standards Drafting Team guidance is one means to align the recommendations herein with the perceived intent of the standard.

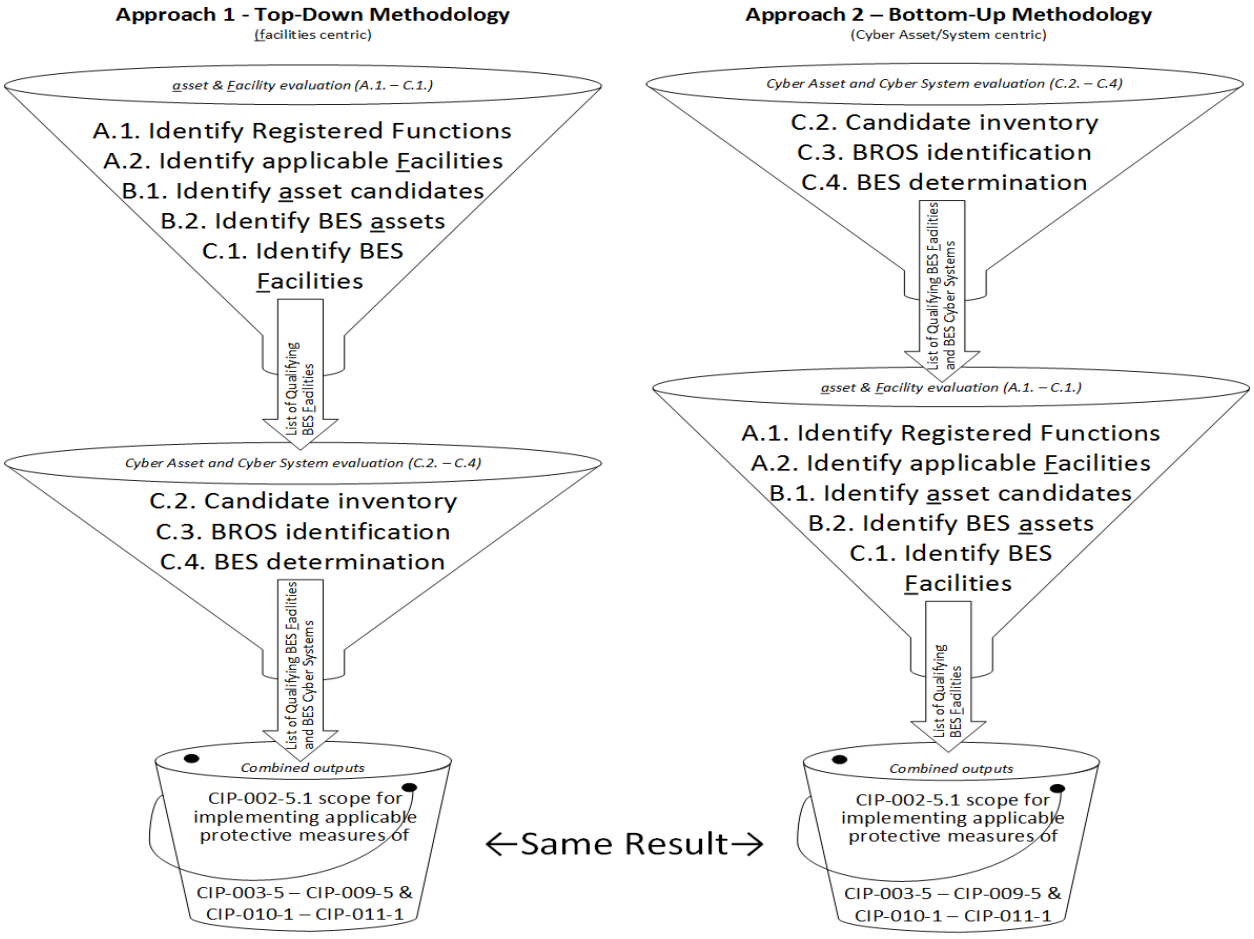
Because various characteristics, factors, and attributes are applied to candidate inventories, it is reasonable to expect that some candidates in either methodology component may qualify for protections whereas other candidates may not. Some examples include, but are not limited to:

- Existence of assets that do not qualify as BES assets.
- Existence of non-BES Facilities that do not meet the Applicability of CIP-002-5.1 and therefore do not require the application of the Attachment 1 criteria that identifies qualifying impact-rated BES Facilities.

- Existence of Cyber Assets that perform a BROS, yet do not qualify as BES Cyber Assets because they do not meet the condition of causing adverse reliability impact within 15-minutes per the BES Cyber Asset definition.
- Existence of Cyber Assets that perform a BROS, yet do not qualify as BES Cyber Assets because they are not associated to a non-BES Facility that qualifies as an impact-rated BES Facility per Attachment 1.

Because each of these two methodological components could be performed independently, it is reasonable to conclude that each would reap the same result regardless of the order in which they are performed. Diagram 1 illustrates the high-level steps of each approach, and the concept that either approach can effectively achieve the intended result.

Diagram 1



Note 1: Step A utilizes the Applicability of CIP-002-5.1, Step B utilizes Requirement R1 of CIP-002-5.1, and Step C is the application of Attachment 1 impact rating criteria. Depending on the assets identified in Step B, Step C.2 could begin with either a candidate inventory of Cyber Assets or a candidate inventory of Cyber Systems. Approach 1 has two variations, each of which achieves the expected result, as detailed in Appendix D.

Note 2: The letter-case of specific terms is deliberate to distinguish between official terms defined in the NERC Glossary of Terms and informal terms used in the context of this guideline. Where a term is NERC-defined, it is capitalized. For Example: Where the intent is to use the NERC-defined term "Facility" it will appear as "Facility." Where the informal term is used, this word will appear as "facility" or "[f]acility."

Tip: When identifying asset candidates, it may be helpful for the entity to think of "facilities" as used above and not as "Facility" in this context defined by NERC ("*A set of electrical equipment that operates as a single Bulk Electric System Element*"), but instead as an asset or "facility containing one or more of the six types of assets listed in CIP-002-5.1 R1." That is, a facility acting as a container for one or more assets. Thinking in these terms will prevent confusion in cases where there may be two types of BES Cyber Systems at one location – for instance a medium impact Special Protection System (SPS) at a low impact substation.

The team recommends the facilities-centric approach. While there are pros and cons to each approach, each entity should weigh its own needs and the unique nature of its systems. The team has written this application guide according to its recommendation. The CIP SME rationale for a facilities-centric approach includes:

- Previous versions of the CIP standards have been based around analysis of facilities ("Critical Assets") so most entities are familiar with this model.
- Lists of facilities and perhaps lists of individual Cyber Assets are typically easily obtainable from an asset management system, but an entity may not as easily be able to compile lists of collections of Cyber Assets grouped by reliability function (BES Cyber Systems) for analysis.
- A BES Cyber System may span multiple facilities. A facility that contains part of a BES Cyber System could easily be over-looked when not first assessing each facility.
- Analysis of facilities should include ALL facilities in order to be complete. When analyzing a facility it should be more straightforward to determine whether it has impact on the BES rather than trying to identify cyber systems that may span across multiple facilities. For example:
    - Example 1 - A facility that merely collects customer payments may have no effect on the BES. This facility should be an easy one to exclude from scope of the CIP standards. This facility would still show up on the list of analyzed facilities and have an explanation as to why it does not fall under the CIP umbrella.
    - Example 2 – A Registered Entity's Main General Office facility may have Cyber Systems that support the BES so this facility would need closer inspection. If there are Cyber Systems that are required for reliable BES operation, these systems need to be analyzed for categorization. A listing of all Cyber Systems at this facility should be listed and analyzed.
    - Example 3 – When a Registered Entity's Transmission Control Center contains BES Cyber Systems, this facility will need to be categorized and a list of BES Cyber Systems will need to be compiled.

- It would be prudent to list all facilities and simply note that a facility "has no high or medium BES Cyber Systems" than to have an incomplete listing of facilities. A thorough and complete list of facilities should help provide reasonable assurance that a thorough analysis has been completed.

Recommended Approach (Approach 1):

CIP-002-5.1 is organized in three (3) sections Applicability, Requirements, and Attachment 1 Impact Rating Criteria. When applying CIP-002-5.1, the recommended methodology is to apply the Standard in the order of these three (3) sections.

Process
Historically, CIP Standards Versions 1-3 involved a BES Asset-based approach where Critical Assets were determined first based on risk, followed by an identification and classification of Cyber Assets.

The recommended approach (Approach 1) employs similar thinking wherein Registered Entities would first determine applicable Entity Function(s) and develop an inventory of facilities. Secondarily, determine the classification of each facility by applying the Impact Rating Criteria in Attachment 1, and conclude with an identification of High and Medium Impact BES Cyber Systems, as well as Low Impact BES Assets.

A. Applicability: *Determining which Functional Entities and Facilities to consider*

This list of candidate Facilities becomes the input to the next step. Begin with a deep review of Section 4 – Applicability within Section A of CIP-002-5.1. Answer these questions and for evidentiary purposes document the results:

1. Am I a functional entity under 4.1?
   a) If yes, document the list of applicable Functional Entities
2. Do I own Facilities[2] under Applicability 4.2?
   a) If yes, document the list of applicable types of Facilities
3. If either of the above is a "Yes", continue. If both of the above are "No", CIP Version 5 is not applicable; however, the recommendation would be for the Registered Entity to document this result.

B. Requirements:

Note: The term **Asset** is used below to mean the following as described on page 17 of the Guidelines and Technical Basis section of CIP-002-5.1:

Asset – Groups of Facilities, systems, and equipment at an identified location or facility. For example, an *asset* may be a named substation, generating plant or Control Center.

[2] Refer to the NERC Glossary of Terms for the definition of "Facility."

Note: It is important to note that there are two posted versions of the standards – one with rationale in-line with the requirements and one with the rationale grouped at the end. Where page numbers are used this refers to the version posted on the CIP Standards page[3] under "Subject to Future Enforcement" where the rationale is grouped at the end.

1. *Preparing the list of BES candidate Facilities*: In an effort to build an initial list of BES candidate assets, the qualifiers within R1 have been removed for this step and those criteria are applied later. From the result in the previous step, document which of the six high level categories in R1 you own. This is your BES candidate list for use in the next step.
    a) Prepare a list of Control Centers and Backup Control Centers
    b) Prepare a list of Transmission stations and substations
    c) Prepare a list of Generation resources
    d) Prepare a list of systems and facilities used for system restoration
    e) Prepare a list of Special Protection Systems[4]
    f) Prepare a list of Protection Systems for Distribution Providers
2. *Considering BES candidates and determining BES Facilities:* From the list of candidates determined in the previous step, mark those that are out of scope. To do so, differentiate between those candidate Facilities that are BES and those that do not qualify as BES.
    a) Remove any Control Centers or Backup Control Centers that do not meet the NERC Glossary definition of Control Center.
    b) Remove any Transmission stations and substations that do not meet the BES definition.

        Note: UVLS and UFLS are subject to CIP-002-5.1, and may be located at assets containing Facilities under 100 kV. Registered Entities are encouraged to incorporate provisions into Step 2.b to assure that applicable UVLS and UFLS are identified and that the Cyber Assets/System candidates are evaluated.

    c) Remove any Generation resources that do not meet the BES definition.
    d) Remove any system restoration systems or facilities that do not meet the NERC Glossary definition of Blackstart Resources or Cranking Paths.
    e) Remove any Special Protection Systems that do not support the reliable operation of the BES.
    f) Remove any Distribution Provider Protection Systems that do not meet the criteria of Applicability 4.2.1.

[3] See http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[4] Refer to the NERC Glossary of Terms for the NERC adopted revised Special Protection Systems (SPS) and Remedial Action Scheme (RAS) definitions

C. Attachment 1: *Performing the Categorization of BES Facilities and Applying the Impact Rating Criteria to BES Cyber Systems*

Tip: For evidentiary purposes, consider retaining two outputs; the first being the list of candidate Facilities with the BES designation of "Yes" or "No" and documentation as to why an asset is in or out of scope, and the second being the list of BES Facilities to use as an input to the next step. The following supplemental worksheets for the practical application are available upon request and are listed in Appendix B: High_impact.xlsx, Medium_impact.xlsx, Low_impact.xlsx, EACMS.xlsx, and PACS.xlsx.

Attachment 1: *Performing the Categorization of BES Facilities and Applying the Impact Rating Criteria to BES Cyber Systems*

1. **Categorizing identified BES Facilities:** Categorize the output from the previous step to those entries that qualify as BES Facilities in sequential steps, using Attachment 1.
    a) Medium (Generation and Transmission facilities criteria 2.1 – 2.10)
    b) High (Control Centers criteria 1.1 – 1.4)
    c) Medium (selected Control Centers criteria 2.11 – 2.13)
    d) Low (Remaining BES Facilities)

    Note: The ordering above is deliberate because of the dependencies between High, Medium, and Low.

    Tip: For evidentiary purposes, consider retaining the output demonstrating the list of BES Facilities and the categorization for each of those BES Facilities in addition to using this result as an input to the next step

2. **BES Cyber Assets**: *Identifying the in scope BES Cyber Assets*

    Establish an inventory of the candidate Cyber Assets for identified assets with High and Medium Impact-Rated BES Facilities in order to determine which meet the criteria of the BES Cyber Asset definition. The terminology varies slightly between High and Medium Impact Criteria therefore this section has been split into two sets of steps to address those variances.

    Note: The steps that follow utilize the concept of a BES reliability operating service, sometimes referred to as "BROS," as described more fully, as an option, in the Guidelines and Technical Basis section of CIP-002-5.1, pages 17-22. Again, it is important to note that there are two posted versions of the standards – one with rationale in-line with the requirements and one with the rationale grouped at the end. Where page numbers are used this refers to the version posted on the NERC

CIP Standards page[5] under Subject to Future Enforcement where the rationale is grouped at the end.

Note: The term, "associated", when used in connection with the Medium Impact-rated Facilities is used to mean the following:

Associated: A mechanism used to focus the list of BES Cyber Assets identified at the Medium Impact Facility to those that are capable of, and purposed for, the performance of one or more BES reliability operating services. Where a system meeting the Medium impact rating criteria is comprised of a collection of geographically dispersed components, like an SPS for example, applicable Registered Entities should give consideration to those geographically dispersed components when determining the associated Cyber Assets that are pertinent to the qualifying Facility.

a) *High BES Cyber Assets*:
   - Using the BES Facilities identified in the previous step, inventory the Cyber Asset candidates at the asset with the High Impact BES Facility.
   - Identify which Cyber Assets meet the criteria for BES Cyber Assets, including the BROS criteria when using that option.

b) *Medium BES Cyber Assets*:
   - Using the BES Facilities identified in the previous step, inventory the Cyber Asset candidates at each asset with the Medium Impact BES Facility.
   - Identify which Cyber Asset candidates meet the criteria for BES Cyber Assets, including the BROS criteria when using that option.
   - Evaluate the inventory of BES Cyber Assets to determine which are associated specifically with each Medium Impact BES Facility.

➢ Because this step in the process involves NERC definitions and several other key considerations, before moving into the next step, the following several pages provide detailed guidance to help assure those considerations are made during the Cyber Asset analysis.

Tip 1: Entities may find it useful to document, during the inventory exercise, the type of connectivity each Cyber Asset uses to aid in evaluating reengineering options and final BES Cyber System determination later in the process. The companion document named Cyber_Asset_Procedure.doc is a sample methodology listed in Appendix B has some examples of Cyber Asset attributes entities may want to consider.

[5] See http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Tip 2: Keep in mind the 15-minute scoping characteristic of a BES Cyber Asset as listed in the NERC Glossary of Terms. Entities should be prepared to demonstrate how they evaluated the 15-minute impact to each BES Cyber Asset as it relates to the consideration of loss, compromise, or misuse. On the inventory worksheets, consider showing both the Cyber Assets that meet the 15-minute definition, and those that do not.

The 15-minute consideration could be related to what actions could be taken by an applicable Reliability Coordinator, Balancing Authority, Transmission Operator, or Generator Operator within 15-minutes to avoid Adverse Reliability Impacts to the BES.

These actions might include, but not be limited to:

- Automatic relay operation
- Operating procedures that do not require the collection, processing, and assessment of system data
- Supervisory control switching of reactive resources
- System reconfiguration using supervisory control
- Fast generation re-dispatch
- Load shedding using supervisory controls

When using the above actions in analyzing the 15-minute impact of a BES Cyber Asset within a System, it is important to note that you cannot use that BES Cyber System itself to mitigate its own risk. This guide talks more about the rationale for the exclusion of redundancy on the next couple of pages.

(As an example, if you're analyzing the 15-minute impact of a substation Cyber System which contains an RTU and protection system relays, and conclude that there is no 15-minute impact as a function of an operator's capability to open some breakers at the substation and re-route around a few of the bus sections if those relays are rendered unavailable, that is unsound by definition because it is using the BES Cyber System to mitigate its own risk, which is explicitly precluded in the NERC BES Cyber Asset definition "…Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact." Conversely, the ability to re-dispatch and control at neighboring substations would be valid where that action is accomplished via a separate BES Cyber System.)

Note that the availability of potential mitigation actions may vary with system operating conditions, such as, system load levels, generation dispatch levels, spinning reserves, area weather conditions, and/or other circumstances.

Registered Entities could decide that Cyber Assets performing a BROS for a high, medium, or low impact - rated Facility requires protections independent of the

15 – minute parameter within the BES Cyber Asset definition. This is another potential approach toward security and compliance.

Registered Entities choosing to consider the 15-minute parameter are advised to document the approach well to provide assurance that it considers necessary aspects that go beyond the absence of a BES Cyber Asset. One potential way to make an assessment is to ask the following question:

> *If a high, medium, or low impact-rated Facility was to be called upon to perform its reliability function, and the successful performance of that function was dependent on a Cyber Asset*, and the Cyber Asset experienced loss, compromise, or misuse resulting in:*
>
> - *an inability of performing its BROS,*
> - *an in ability of performing its control function, or*
> - *compromise and misoperation/malicious operation*
>
> *Would that condition adversely affect reliability within 15 minutes?*

Where a Cyber Asset's absence, mis-operation, or malicious operation would cause a high, medium, or low impact-rated Facility to be incapable of successfully performing it is called upon reliability task or function resulting in adverse impact to reliability within 15 minutes, it would qualify as a BES Cyber Asset with this approach.

An SPS is a good example. Where an SPS becomes unavailable and there is no condition requiring it to perform, there is no adverse impact. However, if the SPS is unavailable when it is called upon, within 15 minutes the adverse impact could be huge and constitute loss. Similarly, if a runback is initiated on the SPS when it is not supposed to be, an adverse impact could occur within 15 minutes due to that misoperation or misuse.

Regardless of approach, to add clarity to individual Entity interpretations, Entities are encouraged to define terms used in their analysis, if not already defined in the NERC Glossary of Terms. Some sample definitions could be:

- **Adverse impact**: A significant harmful effect of an unavailable, degraded, or misused BES Cyber Asset/System that would result in failure of the identified BES Facility to perform its *designed function.*
- **Designed function**: BES Reliability Operating Service or other defined functional obligation(s) or responsibility as documented in the NERC Functional Model[6].

[6] See http://www.nerc.com/pa/stand/pages/functionalmodel.aspx

- **Unavailable**: A point in time or condition when a BES Cyber Asset (for whatever reason and regardless of redundancy) cannot perform its *designed function* or is being operated in a manner for which it was not intended to operate.

***Cyber Asset**: Entities are also advised to exclude redundancy of Cyber Assets when determining if the 15-minute parameter includes or excludes a Cyber Asset because it is typical, and often necessary, for Cyber Assets operating in a redundant mode to be comprised of similar hardware, software, and configuration, making them subject to the similar threats, attack vectors, and vulnerabilities. Though there are a broad range of events or circumstances that could cause a Cyber Asset to become incapable of performing its designed function, it is reasonable to conclude that one reason a Cyber Asset may become incapable could be due to malicious forms of compromise (e.g., viruses, malware, remote code execution, unauthorized access, etc) and, in those scenarios, there is an elevated likelihood that compromise of an individual Cyber Asset operating in a redundant mode may lead to compromise of its counterpart(s) thereby rendering the redundant system incapable as a whole. It is for reasons like, but not limited to, this that Entities should exclude redundancy of Cyber Assets as a factor when performing evaluations to determine criticality to safe, reliable operations.

Tip 3: Where virtualization is concerned, it is important to understand that mixed-trust environments require additional analysis to assure the proper classification is derived and the necessary protective measures are implemented. A "high-watermarking" concept applies to Cyber Assets that share physical infrastructure. Some examples include, but are not limited, to the following:

- A physical Cyber Asset acting as a hypervisor that hosts multiple virtual servers (virtual Cyber Assets)
- A physical Cyber Asset with a shared backplane that transports multiple Virtual Local Area Networks (VLANs)
- A physical Cyber Asset with a shared chassis/backplane that houses multiple interface cards

Scenarios like these have the potential to create a mixed trust environment within a BES Cyber System. The standards allude to a "high-watermarking" concept that precludes mixed trust environments within BES Cyber Systems, such that a Cyber Asset at a lower impact rating is elevated to the highest impact rating with the BES Cyber System to afford it the same protective measures and minimize the risk it may otherwise pose as an attack vector.

Tip 4: Depending on the operational dependencies between BES Cyber Assets within a BES Cyber System, applicable Registered Entities should consider if the local transport/exchange of data between the BES Cyber Assets within the BES Cyber System is integral to the reliable operations of those BES Cyber Assets. Where BES Cyber Assets are dependent on a service, like local network transport, to successfully perform the designed function, the Cyber Asset providing that network transport (redundancy excluded) becomes essential to the reliable operations of the system. As a result, the Cyber Asset(s) that are capable and purposed for providing the transport mechanism within the system becomes a BES Cyber Asset(s) because of its essentiality. Registered Entities are encouraged to evaluate the potential adverse impact related to Cyber Assets of this nature, as not all networking equipment may rise to the level of essentiality necessary for it to become a BES Cyber Asset inside a BES Cyber System, as opposed to a Protected Cyber Asset associated to a BES Cyber System. Potential scenarios include, but are not limited to:

- This concept may be particularly relevant in a typical routable Control Center environment, for example. Within a Control Center environment, it is not uncommon for BES Cyber Assets to be dependent on the ability to communicate with each other over a local area network (LAN). The LAN transport services are essential to the intercommunications between these BES Cyber Assets, and if the networking equipment experienced loss, degradation, or misuse it could result in adverse impact to the BES Cyber Assets that rely upon it, thereby making the networking equipment a BES Cyber Asset.
- This concept may be less relevant in a typical substation environment, for example. Within a substation, it is not uncommon for a BES Cyber Asset to continue to perform its reliability function independent of the LAN and independent of the other BES Cyber Assets within that LAN. Often times, substation devices are connected to a routable network for the convenience of remote management. Where a Cyber Asset is inside an ESP and its capability and purpose provides a non-essential function for the BES Cyber System, that Cyber Asset may be more appropriately classified and secures as a Protected Cyber Asset (PCA) associated to the BES Cyber system.

Every entity is unique, and should identify its own criteria for determining devices that fall into this category where the essentiality of the Cyber Asset to other BES Cyber Assets is a factor in its classification and protective measures.

Tip 5: For evidentiary purposes, consider retaining the input of the Cyber Asset inventory and the output demonstrating the identification of those that qualify as BES Cyber Assets for identified assets with High and/or Medium Impact BES Facilities.

Tip 6: For evidentiary purposes, consider retaining the output demonstrating the full list of BES Cyber Assets at the Medium Impact BES Facility in addition to the documented evaluation as to whether a given BES Cyber Asset is, or is not, associated to the Medium Impact BES Facility.

Note 1: The process of inventorying of all Cyber Assets at a transmission station or substation, and subsequent identification of BES Cyber Assets associated with an identified impact-rated BES Facility at a BES asset may be more practical for criteria that apply to Facilities at substations. However, identifying the BROS first may be especially practical for Control Centers and generation facilities that contain many Cyber Assets and systems that are not pertinent to BES operation. An alternate approach for entities to consider for an asset that contains more than one function beyond the BES reliability operating service (i.e., large facilities with multiple functions, like controls centers or generation facilities) may be to reverse Steps C.2 and C.3 to focus first on the BROS, and next to identify the BES Cyber Assets associated to them. Entities choosing to employ this alternate approach may also want to consider documenting the method used to differentiate between business systems vs. those systems with BES reliability operating services.

Note 2: This approach recommends that entities identify the BROS used by the Facilities that met the Attachment 1 criteria. Another alternate approach is for entities to utilize the BROS as a set of Cyber Asset assessment criteria for with which to use in conjunction with the adverse impact determination and the 15-minute qualifier in order to determine BES Cyber Asset classification. Where entities employ this alternative approach, it may make sense to consider performing Steps C.2 and C.3 simultaneously as opposed to in series. Appendix B includes a companion document (Cyber_Asset_Procedure.doc) that is a sample methodology that employs this approach.

3. **BES Reliability Operating Services**[7]: *Identifying the criteria for subsequent BES Cyber Asset grouping*

   a) *High BES Facilities*:

   - List the reliability tasks for each Registered Entity function using the pre-identified BES reliability operating services[8]
   - Associate each listed task to each identified BES Cyber Asset at the identified asset with High impact Facilities

[7] Refer to the Reliability Operating Service table on page 18 of the Guidelines and Technical Basis section of the NERC Reliability Standard CIP-002-5.1

[8] Id.

b) *Medium BES Facilities*:

- List the reliability tasks for each Registered Entity function using the pre-identified BES reliability operating services[9]
- Associate each listed task to each identified BES Cyber Asset at the identified asset with Medium impact Facilities

Tip 1: For evidentiary purposes, consider retaining the output demonstrating the list of Impact-Rated BES Facilities, each associated Registered Entity function and BES reliability operating service(s), and the corresponding BES Cyber Assets in addition to using this result as an input to the next step.

4. **BES Cyber Systems**: *Applying the Impact Rating Criteria to identify the BES Cyber Systems based on the associated BES Facilities*

Identification of the BES Cyber Systems is accomplished by evaluating the output of the previous step and determining and documenting the BES Cyber Asset groupings:

a) *High and Medium BES Cyber Systems*:

- Evaluate the identified BES reliability operating services for each identified BES Cyber Asset and determine how to group them into one or more BES Cyber System(s).
- Consider engineering revisions to reduce the impact each BES Cyber System has on each BES Facility.
- Identify connectivity characteristics of each identified BES Cyber Asset and each BES Cyber System.
- Evaluate how connectivity characteristics impact the cyber security risk and reliability impact to each identified BES Cyber System.
- Evaluate the topological redesign options to reduce the impact that cyber connectivity factors may have on each BES Cyber System.
- Evaluate the remaining Cyber Assets to determine if they meet the criteria for protection as another classification of Cyber Assets:
  - Electronic Access Point (EAP),
  - Electronic Access Control and Monitoring System (EACMS)
  - Physical Access Control Systems (PACS)
  - Protected Cyber Asset (PCA)
- Determine final inventory of in-scope BES Cyber Assets.

[9] Id.

- Determine placement of Electronic Access Points.
- Document final BES Cyber Systems, impact rating, and associated BES Cyber Asset inventory and connectivity.

b) *Low BES Cyber Systems*:

- Cyber inventory lists are explicitly excluded in the standard; therefore, Low Impact BES Cyber Systems become a list of Low Impact BES Assets that include the list of remaining BES Facilities from Applicability Section 4.2 after the High and the Medium BES Cyber Systems are identified.

A graphical representation of this process can be found in Appendix C.

BES Cyber Systems – Additional Guidance

Definitions from the NERC Glossary of Terms:

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.

BES Cyber Systems concept introduced in CIP-002-5.1: BES Cyber Systems is a new concept introduced by CIP-002-5.1. For the purposes of this Standards Application Guide, the concepts in the CIP-002-5.1 Guidelines and Technical Basis were considered in developing a recommended approach. It is up to each Registered Entity to determine how BES Cyber Assets are grouped into BES Cyber Systems. NERC has provided guidance on potential criteria that be used by Registered Entities to limit the scope of applicable Cyber Assets based on BES reliability operating services. The identification of the applicable Cyber Assets helps lead to the identification of applicable BES Cyber Assets, and in turn leads to the identification of the BES Cyber Systems.

High and Medium Impact BES Cyber Systems: Once the medium and high impact rated Facilities are identified, it is the recommendation that entities begin with the identification of the BES reliability operating service(s) based on the Registered Entity's functions at each identified BES Facility.

Once an entity has identified the reliability operating service(s), entities may want to consider performing an inventory of Cyber Assets at each medium and high impact rated BES Facility to enable a correlation between the two. Once the inventory has been established, each Cyber Asset's function should be considered against the BES Cyber Asset definition to distinguish between those Cyber Assets essential to the reliability of the BES Facility and those that do not qualify by definition. After scoping the Cyber Asset list down to BES Cyber Assets, the next step would be to correlate the applicable reliability operating service(s) and Registered Entity Function(s).

Once BES Cyber Assets are associated to the BES reliability operating service(s), BES Cyber Assets can be placed into logical groupings to define initial BES Cyber System(s).

Tip: Because each Cyber Asset may support more than one BES reliability operating service, it is possible for a given Cyber Asset to be part of more than one BES Cyber System. It is the recommendation to identify all applicable BES reliability operating services so that future operational changes or changes in registration of the functional entity do not lead to oversights that cause BES Cyber Assets to inadvertently fall off the list.

When determining BES Cyber Asset inventories and initial groupings into BES Cyber Systems entities may encounter situations where the connectivity between BES Facilities or BES Cyber Assets draws into scope other Facilities or Cyber Assets that were not previously identified. Through the consideration of reengineering or topological design, entities may have options to architect the infrastructure to focus the scope.

The BES Cyber System grouping may also be 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 an entity groups Protection Systems at a number of stations or substations into a single BES Cyber System, the communications network connecting them will need to be considered within the scope of the CIP standards. If the various Protection Systems identified as BES Cyber Systems need to meet the same CIP standard Requirements, there is 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 levels (i.e., 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 suitable approach.

For High and Medium Impact-rated BES Cyber Systems, it may be difficult to finalize BES Cyber System identifications without stepping outside of CIP-002-5.1 because of the potential for multiple Facilities to co-exist at an single BES asset location, in addition to connectivity factors that must be given consideration. Subsequent to the initial determination of BES Cyber System(s), an entity may want to perform an evaluation to consider engineering revisions that reduce the impact that each BES Cyber System has on each Facility. Reengineering considerations include, but are not limited to:

1. Identification of higher impact BES Facilities that co-exist with lower impact BES Facilities.
2. Operational separation of the higher impact BES Facilities from lower impact BES Facilities.
3. Physical separation of the higher impact BES Facilities from lower impact BES Facilities.

In addition, an entity may want to identify connectivity characteristics for each identified BES Cyber Asset in order to reduce the security risk that each identified BES Cyber System has on each BES Facility. Connectivity considerations include, but are not limited to:

1. Identification of External Routable Connectivity and Electronic Access Points.
2. Identification of Dial-up Connectivity for each BES Cyber System.
3. Identification of the BES Cyber Asset(s) that establish a high-water mark, which is a concept wherein Cyber Assets interconnected within logical environments containing

BES Cyber Assets require elevation to the highest impact level of the BES Cyber System. For example, a relay assessed to be part of a Medium Impact BES Cyber System is routably connected to a relay that does not perform a function that would qualify it to be part of a Medium Impact BES Cyber System. In this case, the entity might consider an engineering re-design that would involve a removal of that routable connection.

4. Identification of the topology or interconnectivity with other Cyber Assets at the Facility that do not meet the criteria of the BES Cyber Asset definition (A.K.A. Protected Cyber Assets).

Once a Registered Entity understands the BES Facility engineering as well as the connectivity between Cyber Assets, consideration may be given toward topological redesign to reduce the impact that cyber connectivity factors may have on each BES Cyber System. Potential topological redesign considerations include but are not limited to:

1. Logical separation/segmentation of the higher impact BES Cyber Assets from lower impact BES Cyber Assets.
2. Logical separation/segmentation of Cyber Assets that do not qualify as BES Cyber Assets.
3. Elimination of any External Routable Connectivity that is not required for the reliable operation of the BES.
4. Elimination of any Dial-up Connectivity that is not required for the reliable operation of the BES.
5. Elimination of any Interactive Remote Access that is not required for the reliable operation of the BES.

Subsequent to these activities, entities should finalize the inventory of in-scope BES Cyber Assets and determine placement of Electronic Access Points, while maintaining the association each BES Cyber Asset has with the identified BES reliability operating services and Registered Entity Function(s). This data in combination allows for the final identification and categorization of high and medium impact-rated BES Cyber Systems.

Naming Considerations: Registered Entities may also want to consider documenting a predefined naming convention to represent each BES Cyber System association. One way an entity might identify its BES Cyber Systems is to combine all of the attributes that were considered throughout the methodology that led to the identification of a BES Cyber System. The level of granularity in naming each BES Cyber System is up to each entity. It is the recommendation to implement as much granularity as is necessary to fully qualify and clearly define the boundaries of each identified BES Cyber System. Where an entity decides to use abbreviations, it is the recommendation that documented definitions or explanations of those abbreviations or acronyms accompany the methodology and the associated output. Here are some examples of potential naming conventions:

1. Registered Entity Function + BES reliability operating service + BES Facility name
    - BA– BES Restoration – City Y Control Center
    - BA_BESR_ CityYCC
2. Registered Entity Function + BES Impact Rating + BES reliability operating service + subservice + BES Facility name
    - TOP - Medium Impact – Balancing Load and Generation – Demand Response – City Y Substation
    - TOP_Med_BL&G_DR_ CityYSub

Low Impact BES Cyber Systems: BES Cyber Asset inventory lists and grouping them into BES Cyber Systems is explicitly excluded in the standard; therefore, Low Impact BES Systems become a list of Low Impact BES Assets that include the list of remaining BES Facilities from Applicability Section 4.2 after the High and the Medium BES Cyber Systems are identified.

However, at the time of this writing, revisions to CIP-003-5 are being finalized that would put additional requirements onto Low Impact Cyber Systems. While not explicitly required by the standard, Registered Entities would be best served having an inventory of such systems so that they can ensure the proper controls are placed on all of them.

Evaluating CIP-002-5.1, Requirement 1

CIP-002-5.1 replaces the Risk Based Assessment Methodology in CIP-002-3 with the impact rating criteria in an attachment to CIP-002-5.1. Understanding the scope of version 5 in your entity is essential to meet these new requirements. The MRO CIP SME Team provides this methodology as one possible approach to document the requirements. These recommendations do not provide an officially approved set of evidence, but believes this process will meet requirements of most organizations.

> ***R1:*** *Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning]*
>
> ***i.*** *Control Centers and backup Control Centers;*
> ***ii.*** *Transmission stations and substations;*
> ***iii.*** *Generation resources;*
> ***iv.*** *Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;*
> ***v.*** *Special Protection Systems that support the reliable operation of the Bulk Electric System; and*
> ***vi.*** *For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.*

Analysis

- Per the guidance provided in the Guidelines and Technical Basis section of CIP-002-5.1 and where the CIP Version 5 drafting team uses the term "Facilities," there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

- The Time Horizons for Requirements R1 and R2 are Operations Planning. Per NERC, the Operations Planning Time Horizon is from the Day-Ahead to the Seasonal Time Horizons.[10]
  a. The specific time range of the Operations Planning time horizon is vague and undefined, so a working range of next day to 18 months into the future is suggested, when it can be applied.
  b. Note that Impact Rating Criterion 2.1 is based on the preceding 12 months of historical data. So the evaluation of this criterion must be timed to be completed just before the 2.1 assessment is completed.
  c. Note that Impact Rating Criteria 2.3 and 2.6 are based on Planning Coordinator and Transmission Planner evaluations. The evaluations of these functional entities apply for the Long-Term Planning horizon (e.g., 1 to 10 years into the future), which extends beyond the Operations Planning horizon. It is suggested that these criteria be evaluated for Year 1 and 2 of the Long-Term Planning horizon. This approach would allow for the identification of new facilities up to two years before they will be placed in service and up to two years to implement (e.g., design, procure, and install equipment to meet) any resulting compliance obligations.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- Per the guidance provided in the Guidelines and Technical Basis section of CIP-002-5.1, each BES Cyber System should be listed and classified by only one Responsible Entity. When applicable BES Cyber Systems or BES Facilities are owned jointly with other entities, then it is suggested the joint owners reach an agreement with the other owners regarding who will determine the Impact Rating of BES Cyber Systems or Facilities, systems, and equipment. It is also suggested that entities normally agree on having the majority owner be the entity who will determine the Impact Rating.

Tip for Requirement 1:

1. If the Impact Ratings list is null, then clearly document that the list is null.
2. Include the name of the preparer and approver, as well as the date on all critical and supporting evidence documents.

Critical Evidence:

A list of Facilities requiring assessment and the one-line diagrams for those assessments

[10] See http://www.nerc.com/files/Time_Horizons.pdf

For consistency across the NERC Standards, Table 1 provides a list of resources a Registered Entity may already have that can act as an input to the six assets in Requirement R1.i – vi, and those sources that may be evidence that may be required to demonstrate compliance. While inputs to CIP-002-5.1 Requirement R1 may be produced through compliance with other standards, entities may want to consider providing those records. All other requirements are addressed by separate evidence the Registered Entity is required to maintain for other standards.

Table 1. Suggested List of Inputs for Impact Analysis

This table is intended to support the identification of assets to be considered as part of the entity's CIP-002-5.1 assessment. Compliance with other operations reliability standards may result in lists of assets that could be leveraged to ensure completeness in the entity's CIP-002-5.1 asset inventories.

Functional Registration • Documentation or attestation of NERC Functional Registrations for the Registered Entity

BES Assets and other assets in scope for evaluation
• List of BES Assets in accordance with the NERC BES definition. All Blackstart assets are included in the BES definition.
• If a Distribution Provider, the following assets are required to be evaluated (see Applicability Section 4.2.1).
  o Automatic UFLS or UVLS Programs.
  o Assets with Special Protection Systems/Remedial Action Schemes.
  o Transmission Assets subject to one or more NERC standards.
  o Cranking Paths and Elements from a Blackstart Resource.

One-line diagrams • One-line diagrams depicting all BES Assets and other assets in scope   o Include generation interconnection diagrams • FAC-008-3 R8.1.1 Facility Ratings provided to RC or TOPs associated with the one-line diagrams
Real Power Capability and Reactive Power Capability • MOD-025-2 Attachment 2 for BES generation Facilities or similar evidence; or • Attestation of no generation and/or no Reactive Power in scope of standard
Special Protection Systems/Remedial Action Systems (SPS/RAS) • PRC-015-0 R1 List of SPS's; or • Attestation of no SPS's

BES Adverse Reliability Impact – Generation • TPL-003-2a – Assessment with finding that a generation Facility is designated as must-run to prevent a category C or higher contingency; or • Attestation of Facilities with no identified BES Adverse Reliability Impact
Interconnection Reliability Operating Limits (IROL) • FAC-014-2 R4 – IROLS (List of Facilities associated with IROLs); or • FAC-014-2 R5 – Received IROL notifications (List of Facilities associated with IROLs); or • Attestation of Facilities with no IROLs & no notification of IROLs received
Under-Voltage and Under-Frequency Load Shed (UVLS & UFLS) • PRC-006-1 R6 UFLS data (document Facilities with UFLS); and • PRC-010-0 R1 UVLS Assessment data (document Facilities with UVLS)
Nuclear Plant Interface Requirements (NPIR) • NUC-001-2 R1 NPIR notifications or NUC-001-2 R2 NPIR agreements; or • Attestation for sites not subject to NPIRs

Attestations are typically considered the weakest form of evidence that can be used to demonstrate compliance. In some cases, use of an attestation may be the only option. While the MRO CIP SME Team cannot definitively state when use of an attestation is acceptable, the entity may want to consider using attestations to document facilities that do not contain items identified in the impact rating criteria.

While other evidence is preferred and may be available, example criteria that may be considered for potential attestation includes:

- Functional Registrations
- Generation Facilities not having an Adverse Reliability Impact
- Facilities not included in Restoration Plans
- Facilities not containing Special Protection Systems
- Facilities not subject to IROLs
- Facilities not subject to Nuclear Plant Interface Requirements
- Facilities with no UVLS/UFLS Systems
- Facilities not participating in multi-Facility load-shed systems
- Control Centers, where those control centers do not perform activities associated with Reliability Coordinator, Balancing Authority, Transmission Operator, and Generation Operator Functional Registrations

Documentation Suggestions

- Retain critical and supporting documentation for a full audit cycle
- For Functional Registration, keep a copy of each version of the NERC or MRO Functional Registration

Evaluating CIP-002-5.1, Requirement R1.1

R1.1. *Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;*

Attachment 1, Section 1, covers the identification of BES Cyber Systems are a High Impact Rating. The High Impact Rating is only associated with BES Cyber Systems that are used by and located at certain Control Centers. It is recommended that each Registered Entity begin the Section 1 assessment by collecting information about its primary and backup Control Centers.

Since the identification of the control centers draws from assets that meet certain Medium Impact ratings (2.1 through 2.10). The Medium Impact Rating assessment should be performed before the High Impact Rating assessment.

The High Impact Rating (1.1 through 1.4) criteria need to be considered by NERC registered Reliability Coordinators (RC), Balancing Authorities (BA), Generator Owners (GO), Transmission Owners (TO), and Distribution Providers (DP) that own Controls Centers or backup Control Centers. Entities must obtain the classification of the Facilities they control from the applicable TO(s), GO(s), and/or DP(s) to assure high impact Control Centers are identified.

- List of Control Centers: Update a list of all Registered Entity-owned Controls Centers or backup Control Centers that are presently in service. Additionally, Registered Entities may want to consider initial evaluation of Control Centers that are planned to be in service within the next two years.
- Determine Control Centers Functional Obligations: Determine whether any of the Control Centers or backup Control Centers perform the functional obligations of a BA, RC, GOP, or TOP. (There are control center worksheets in the CIP-002-5.1 Workbook (Tables C1) that may be helpful for determining each control center's applicable characteristics and functionality.)

Note: The high impact rating criteria in Attachment 1 specifically emphasizes functional obligations, and relies on functional model relationships in addition to registered function.

A Registered Entity may not be registered as a BA, RC, GOP, or TOP, but as a result of a relationship or operating agreement may perform the functional obligations of one of those registrations. Where these relationships or agreement exists, the owner of the Control Center or Backup Control Center is subject to determining whether the asset is categorized as high impact.

For example, a Registered Entity that may be registered as a TO, but through an agreement with another entity may perform TOP functional obligations on behalf of the other Registered Entity. In this case, the owner of a Control Center or a Backup Control Center may need information from the TO in determining whether the control center or backup control center is used to perform the functional obligations of a TOP for one or more assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8. 2.9, or 2.10.

Note: Depending on the logical connectivity of Cyber Asset**s** within an identified BES Cyber System(s), other Cyber Assets beyond the identified BES Cyber Assets may qualify for protection under the CIP Version 5 Standards.

CIP-002-5.1 - Attachment 1

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

Criterion 1.1 *Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.*

Applicability: Reliability Coordinator

- Control Center Identification: Identify and list each Control Center and backup Control Centers that are used to perform the functional obligations of the Reliability Coordinator.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets used by and located at the identified Control Centers and backup Control Centers used to perform the applicable reliability operating services. These services are Balancing Load & Generation, Managing Constraints, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Criterion 1.2 *Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.*

Applicability: Primarily Balancing Authority

- Control Center Identification: Identify the Transmission Owners and/or Distribution Providers who own Facilities that are operated by each Registered Entity-owned Control Center or backup Control Center. Next, ask the identified Transmission Owners and/or Generator Providers whether any of the controlled Facilities meet Attachment 1, criteria 2.3, 2.6, or 2.9. Identify and list the Control Centers and backup Control Centers that are used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criteria 2.3, 2.6, or 2.9.

- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets used by and located at the identified Control Centers and backup Control Centers used to perform the applicable reliability operating services. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Criterion 1.3 *Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.*

Applicability: Primarily Transmission Operator

- Control Center Identification: Identify the Transmission Owners and/or Distribution Providers who own Facilities that are operated by each Registered Entity-owned Control Center or backup Control Center. Next, ask the identified Transmission Owners and/or Distribution Providers whether any of the controlled Facilities meet Attachment 1, criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10. Identify and list the Control Centers and backup Control Centers that are used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets located at the identified Control Centers and backup Control Centers used to perform the applicable reliability operating services. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, Managing Constraints, Monitoring and Control, Restoration, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Criterion 1.4 *Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.*

Applicability: Primarily Generator Operator

- Control Center Identification: Identify the Generator Owners who own Facilities that are operated by each Registered Entity-owned Control Center or backup Control Center. Next, ask the identified Generator Owners whether any of the controlled Facilities meet Attachment 1, criteria 2.1, 2.3, 2.6, or 2.9. Identify and list the Control Centers and backup Control Centers that are used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criteria 2.1, 2.3, 2.6, or 2.9.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets used by and located at the identified Control Centers or backup Control Centers used to perform the applicable reliability operating services. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Managing Constraints, Monitoring and Control, Restoration, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Suggested Critical Evidence for Criterion 1.1 – 1.4:

1. List of Controls Centers and backup Control Centers that meet one or more of the High Impact Ratings criteria and include which criteria were met.
2. List of BES Cyber Systems that have a High Impact Rating due to Criterion 1.1 through 1.4.

Suggested Supporting Evidence for Criterion 1.1 – 1.4:

1. List of Registered Entity-owned Control Centers and backup Control Centers.
2. Lists of identified Cyber Assets that met one or more of High Impact Rating criteria, including which criteria were met.

Evaluating CIP-002-5.1, Requirement R1.2

R1.2. *Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and*

Attachment 1, Section 2, covers the identification of BES Cyber Systems that are a Medium Impact Rating. The Medium Impact Rating is associated with BES Cyber Systems that are associated with applicable Generation Resources, Reactive Power Resources, Transmission Substations, Special Protection Systems, Protection Systems, and Facilities critical to System Restoration. Supplemental worksheets named Attachment1_Worksheets.doc are listed in Appendix B.

CIP-002-5.1 - Attachment 1

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

Criterion 2.1 *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*.

Applicability: Generator Owners

- List of Generation Groups: Identify and list the groups of commissioned generating units that are Registered Entity-owned, that are at single plant locations in a single Eastern, Western, and/or ERCOT Interconnection, and that are presently in service or expected to be in service within the next 12-24 months. Each group must have at least one BES generating unit and will include all of the BES and any non-BES generating units at the single location.
- Determine Aggregate Real Power Capability: Determine the aggregate highest rated net Real Power capability of the preceding 12 calendar months for each combination of applicable generating units and whether any groups have a maximum aggregate capability equal to or greater than 1500 MW. For future units, a conservative consideration may be to use the highest net design Real Power capability.
- Apply 1500 MW Criteria: Identify and list the groups of generating units the meet or exceed the 1500 MW threshold.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation,

identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Controlling Voltage, and Inter-Entity Coordination.

- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets. Determine whether shared BES Cyber Systems could, within 15 minutes, adversely impact the reliability of 1500 MWs or more of aggregate unit capabilities.

Suggested Critical Evidence for Criterion 2.1:

1. List of BES Cyber Systems associated with each group of applicable generation units and the analysis or rationale for determining whether each BES Cyber System could, within 15 minutes, adversely impact the reliable operation of any applicable combination of units.
2. List of BES Cyber Systems that have a Medium Impact Ratings based on Criterion 2.1.

Suggested Supporting Evidence for Criterion 2.1:

1. List of all applicable groups of commissioned generation at all single plant locations and the maximum aggregate capability of the generating units in the group.
2. List of groups of generation with maximum aggregate capability of 1500 MW or more.
3. List of candidate Cyber Assets and identified BES Cyber Assets that are associated with any of the generating units in the groups with a maximum aggregate capability of 1500 MW or more.

Criterion 2.2 *Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). 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 resources that in aggregate equal or exceed 1000 MVAR.*

Applicability: Transmission Owners

- List of Reactive Resource Groups: Identify and list all BES reactive resources, or group of resources (e.g., capacitor banks, inductor banks, power electronic reactive power compensators), at a single transmission location that are Registered Entity-owned and that are either presently in service or expected to be in service within the next 12-24 months. Include the aggregate net Reactive Power nameplate rating of the reactive resources at each single location in the list.
- Determine Aggregate Reactive Power Rating: Identify and list any reactive resources at a single transmission location that exceeded the aggregate rating threshold of 1000 MVAR.

- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services for the identified Reactive Resources. Determine whether shared BES Cyber Systems could within 15 minutes result in the loss of 1000 MVAR or more of reactive resources. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Suggested Critical Evidence for Criterion 2.2:

1. Lists of BES Cyber Systems associated with each group of applicable reactive resources and the analysis or rationale for determining whether each BES Cyber System could, within 15 minutes, adversely impact the reliable operation of any applicable reactive resources.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.2

Suggested Supporting Evidence for Criterion 2.2:

1. Lists of applicable BES reactive resources at a single transmission location as supporting evidence.
2. Tabulations of any reactive resources at a single transmission location that exceeded the aggregate rating threshold of 1000 MVAR as supporting evidence.
3. Lists of candidate Cyber Assets and identified BES Cyber Assets that are associated with one or more of Medium Impact Rating criteria as supporting evidence, including the criteria that are associated with each of the listed Cyber Assets.

Criterion 2.3 *Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.*

Note: The consideration of this criterion needs to be supported by the applicable Planning Coordinator or Transmission Planner.

Applicability: Generator Owners and Generator Operators with support from NERC registered Planning Coordinators and Transmission Planners

- List of candidate Generation Facilities: Identify and list all Registered Entity-owned generation Facilities with BES generating units that are Registered Entity-owned that are presently in service or planned to be placed in service within the next 24 months.
- Adverse Reliability Impacts: Solicit a statement from each associated Planner Coordinator and Transmission Planner regarding whether they designate any of your generation facilities are necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year. Include the list of BES generation facilities in the solicitation.
- Generation Facilities: Evaluate the Planner Coordinator and Transmission Planner responses and determine whether any of your generation Facilities are necessary to avoid an Adverse Reliability Impact in the planning horizon within the next 24 months.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services for the identified Generation facilities. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Controlling Voltage, Managing Constraints, Monitoring and Control, Restoration, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Applicability: Planning Coordinator and Transmission Planners (Compliance obligations for PCs and TPs are identified in TPL-001-4)

- List of Generating Facilities: Update the list of generating Facilities with at least one BES generation unit that are interconnected to your transmission system and are either in service or expected to be in service within the next 12-24 months.
- Evaluate Adverse Reliability Impacts: Evaluate whether any of the generating Facilities on your list are necessary to avoid BES Adverse Reliability Impacts and should be designated as applicable to Criterion 2.3.
    - Perform planning horizon “must run” evaluations (e.g., the loss of all generating units at a single generating facility and each more severe Category B1, B2, and/or B3 contingency). When TPL-001-4 Requirement R4 becomes effective on 1/1 2016, the results of performing the steady state extreme event contingency 2.d will be available to share with the GO upon request.
    - Consider critical system conditions and study years (e.g., year 1 and/or year 2, peak system load).

- Evaluate against the applicable Adverse Reliability Criteria (e.g., voltage instability, uncontrolled system separation, and loss of firm load).

- Inform the Generator Owners or Generator Operators: Inform the Generator Owners or Generator Operators of the generating Facilities on its list regarding which are designated as necessary to avoid BES Adverse Reliability Impacts.

Suggested Critical Evidence for Criterion 2.3:

1. Communications (e.g., letter, email) from each Planning Coordinator and Transmission Planner regarding whether they designated any of your generation facilities are necessary to avoid an Adverse Reliability Impact.
2. Evaluations of whether any of your generation facilities are necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
3. Lists of BES Cyber System(s) that have a Medium Impact Rating due to Criterion 2.3.

Suggested Supporting Evidence for Criterion 2.3:

Generation Owners

1. Lists of the Registered Entity-owned generation facilities with BES generating units as supporting evidence.
2. Attestation from each Planning Coordinator(s) and/or Transmission Planner(s) in cases where no generation facilities qualify for Criterion 2.3.
3. Solicitations of information from your PCs and TPs as supporting evidence.
4. List of candidate Cyber Assets and identified BES Cyber Assets.
5. Lists of BES Cyber Systems associated with the list of applicable generation Facilities as supporting evidence.

Planning Coordinators and Transmission Planners

1. Lists of applicable generation Facilities interconnected to your system as supporting evidence.
2. Evaluations of applicable generation Facilities as supporting evidence.
3. Communications to applicable Generator Owners as supporting evidence.

Criterion 2.4 *Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.*

Applicability: Transmission Owners

- List of Transmission Facilities: Identify and list of all transmission Facilities that are presently operated at 500 kV or higher that are Registered Entity-owned and either are presently in service or expected to be in service within the next 12-24 months.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services for the identified Transmission facilities. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Suggested Critical Evidence for Criterion 2.4:

1. Lists of all transmission facilities that are presently or planned to be operated at 500 kV or higher.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.4.

Suggested Supporting Evidence for Criterion 2.4:

1. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the list of applicable transmission Facilities as supporting evidence.

Criterion 2.5 *Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.*

Voltage Value of a Line	*Weight Value per Line*
less than 200 kV (not applicable)	*(not applicable)*
200 kV to 299 kV	*700*
300 kV to 499 kV	*1300*
500 kV and above	*0*

Applicability: Transmission Owners

- Multiple Line Identification: Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation. For additional information, refer to page 28 of the Guidelines and Technical Basis[11] of CIP-002-5.1.
- List of Candidate Stations: Update a list of all stations and substations and the other station(s) or substation(s) that are connected at 200 kV or higher voltages that are Registered Entity-owned and that are either presently in service or expected to be in service within the next 12-24 months. Include in the list the lines that are connected to other substations at 200 kV to 299 kV and 300 kV to 499 kV.
- Determine Aggregate Weighted Value: Calculate the aggregate weighted value of each applicable station or substation and identify the transmission Facilities any the stations(s) or substation(s) whose weighted value exceeds the 3000 threshold.
- Transmission Facility Identification: Identify and list the Transmission Facilities that that are operating between 200 kV and 499 kV at any applicable station or substation. These Facilities are line circuits and transformer circuits if at least two windings are operated between 200 kV and 499 kV. The line terminals that are located at non-applicable stations or substations are not included.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services for the identified Transmission facilities. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Suggested Critical Evidence for Criterion 2.5:

1. Lists of Transmission Facilities at all stations or substations whose aggregated weighted value exceeds the 3000 threshold.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.5.

[11] See http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Suggested Supporting Evidence for Criterion 2.5:

1. List of candidate stations or substations with number of connected stations and substations, list of applicable lines, and aggregate weighted value of each station or substation.
2. List of applicable stations or substation.
3. List of applicable Transmission Facilities.
4. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the list of applicable transmission Facilities as supporting evidence.

Criterion 2.6 *Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.*

This criterion needs to only be considered for generation at a single plant location by NERC registered Generator Owners and for Transmission Facilities at a single station or substation location by NERC registered Transmission Owners. The consideration of this criterion needs to be supported by NERC registered Reliability Coordinators, Planning Coordinators and Transmission Planners.

Applicability: Generation Owners

- List of Candidate Generation Facilities:
    - Solicit a list from each of its Reliability Coordinators of all Registered Entity-owned generation at single plant locations that it is Reliability Coordinators(s) identified as critical to the derivation of operating horizon Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
    - Solicit a list from each of its Planning Coordinators and Transmission Planners of all Registered Entity-owned generation at single plant locations that it is Planning Coordinators(s) and Transmission Planners(s) identified as critical to the derivation of planning horizon IROLs and their associated contingencies.
- Generating Facility Identification: Evaluate whether the identifications of the RCs, PCs and TPs are truly applicable to Criterion 2.6.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services for the identified generation units. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Controlling Voltage, and Inter-Entity Coordination.

- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Applicability: Transmission Owners

- List of Transmission Facilities:
    - Solicit a list from each of its Reliability Coordinators of all Registered Entity-owned Transmission Facilities at a single station or substation location that it's RC(s) identified as critical to the derivation of operating horizon IROLs and their associated contingencies.
    - Solicit a list from each of its Planning Coordinators and Transmission Planners of all Registered Entity-owned Transmission Facilities at a single station or substation location that it's PCs and TPs identified as critical to the derivation of planning horizon IROLs and their associated contingencies.
    - Evaluate whether the identifications of the RCs, PCs and TPs are truly applicable to Criterion 2.6.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more of these BES reliability operating services for the identified Transmission facilities. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Identify and list the BES Cyber Systems that include the identified Cyber Assets.

Applicability: Reliability Coordinators

- List of Operating Horizon IROLs: Update a list of operating horizon IROLs that either are presently in effect or expected to be in effect within the next 12-24 months.
- List of Critical Facilities to Operating Horizon IROLs: Evaluate whether any of the generation at a single plant location or Transmission Facilities at a single station or substation location is deemed critical to the derivation of operating horizon IROLs and their associated contingencies.
- Inform any Generator Owners of the generating Facilities deemed to be critical to the derivation of operating horizon IROLs and their associated contingencies.
- Inform any Transmission Owners of the Transmission Facilities deemed to be critical to the derivation of operating horizon IROLs and their associated contingencies.

Applicability: Planning Coordinator and Transmission Planners (not a mandatory compliance obligation)

- List of Operating Horizon IROLs: Update a list of planning horizon IROLs that either are presently in effect or expected to be in effect within the next 12-24 months.
- List of Critical Facilities to Operating Horizon IROLs: Evaluate whether any of the generation at a single plant location or Transmission Facilities at a single station or substation location are deemed critical to the derivation of planning horizon IROLs and their associated contingencies.
- Inform any Generator Owners of the generating Facilities deemed to be critical to the derivation of planning horizon IROLs and their associated contingencies.
- Inform any Transmission Owners of the Transmission Facilities deemed to be critical to the derivation of planning horizon IROLs and their associated contingencies.

Suggested Critical Evidence for Criterion 2.6:

1. Generator Owners - Communications from RCs, PCs, and TPs that identify Registered Entity-owned generation facilities as critical to the derivation of IROLs and their associated contingencies.
2. Generation Owners - Lists of BES Cyber Systems that were classified as Medium Impact Facilities due to Criterion 2.6.
3. Transmission Owners - Communications from RCs, PCs, and TPs that identify Registered Entity-owned Transmission Facilities as critical to the derivation of IROLs and their associated contingencies.
4. Transmission Owners - Lists of BES Cyber Systems that were classified as Medium Impact Facilities due to Criterion 2.6.

Suggested Supporting Evidence for Criterion 2.6:

1. Generator Owner - Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the list of applicable generation Facilities as supporting evidence.
2. Transmission Owner - Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the list of applicable Transmission Facilities as supporting evidence.
3. Reliability Coordinator - Lists of operating horizon IROLs and the generation facilities and transmission facilities are deemed critical to the derivation of planning horizon IROLs and their associated contingencies as supporting evidence.
4. Reliability Coordinator - Communications that were sent to GOs, and TOs and identified the respective facilities it deemed critical to the derivation of planning horizon IROLs and their associated contingencies as supporting evidence.

5. Planning Coordinator and Transmission Planners - Lists of operating horizon IROLs and the generation facilities and Transmission facilities are deemed critical to the derivation of planning horizon IROLs and their associated contingencies as supporting evidence.
6. Planning Coordinator and Transmission Planners - Communications that were sent to GOs, and TOs and identified the respective facilities it deemed critical to the derivation of planning horizon IROLs and their associated contingencies as supporting evidence.
7. Attestation from each Reliability Coordinator(s), Planning Coordinator(s) and/or Transmission Planner(s) in cases where no Facilities critical to the derivation of an IROL qualify for Criterion 2.6.

Criterion 2.7. *Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.*

Applicability: Transmission Owners

- List of Nuclear Plant Interface Coordination Agreements: Update a list of all Nuclear Plant Interface Coordination Agreements that were established for compliance with the NUC-001 Reliability Standard and either are presently in effect or expected to be in effect within the next 12-24 months.
- List of Transmission Facilities: Update a list of Transmission Facilities that are Registered Entity-owned and that are identified in any agreements as essential for meeting the NPIRs.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the identified Transmission Facilities. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.7.

Suggested Critical Evidence for Criterion 2.7:

1. Lists of Registered Entity-owned transmission Facilities that are identified in the agreement as essential for meeting the NPIRs.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.7.

Suggested Supporting Evidence for Criterion 2.7:

1. Lists of active and planned Nuclear Plant Interface Coordination Agreements.
2. The Nuclear Plant Interface Coordination Agreements that apply for the last 5 years.
3. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the list of applicable transmission Facilities as supporting evidence.

Criterion 2.8. *Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.*

Applicability: Transmission Owners

- List of Generation Facilities: Solicit lists of generation Facilities from any Generator Owners that are interconnected to its transmission system and have been identified as the result of its application of Attachment 1, criterion 2.1 or 2.3.
- List of Transmission Facilities: Update a list of Transmission Facilities that are required to connect the output of the identified generation to its transmission system that are Registered Entity-owned and either are presently in service or expected to be in service within the next 12-24 months.
- Evaluate whether any of its Transmission Facilities are required to connect the generation output that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3 and update a list of transmission Facilities that meet this criterion.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the identified Transmission Facilities. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.8.

Applicability: Generator Owners (not a mandatory compliance obligation)

- List of Generation Facilities: Provide a list of the generation Facilities that it identified as a result of its application of Criterion 2.1 or 2.3 to any Transmission Owners that own transmission Facilities which connect the generator output to the TO's transmission system.

Suggested Critical Evidence for Criterion 2.8:

1. Transmission Owner - Lists of Transmission Facilities are required to connect the generation output that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.
2. Transmission Owner - Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.8.

Suggested Supporting Evidence for Criterion 2.8:

1. Transmission Owner - Communications (e.g., letter, email) from each Generator Owner regarding any identified generation Facilities as a result of its application of Criterion 2.1 or 2.3.
2. Transmission Owner - Lists of Transmission Facilities that are required to connect the output of the identified generation to its transmission system.
3. Transmission Owner - Lists of candidate Cyber Assets and identified BES Cyber Assets that are associated with the applicable Transmission Facilities.
4. Generator Owner - Communications of lists of generation Facilities that were sent to Transmission Owners in which the Generation Facilities associated with Medium Rating Cyber Systems were identified.

Criterion 2.9. *Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.*

Applicability: Generation Owners that have SPSs, RASs or automated switching systems that operate BES elements

- List of candidate SPS, RASs or Automated Switching Systems: Update a list of all Registered Entity-owned SPSs, RASs or automated switching systems that operate BES elements and that are either presently in service or expected to be in service within the next 12-24 months.

- SPS, RASs or Automated Switching Systems Identification: Determine whether any of the listed SPSs, RASs or automated switching systems would cause one or more IROL violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable. Identify and list the applicable systems. For systems that have elements at multiple substation locations, identify and list the substations, which contain a portion of the applicable system that would cause one or more IROL violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the identified SPSs, RASs or automated switching systems. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Controlling Voltage, and Inter-Entity Coordination.
- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.9.

Applicability: Transmission Owners that have SPSs, RASs or automated switching systems that operate BES elements

- List of candidate SPS, RASs or Automated Switching Systems: Update a list of all Registered Entity-owned SPSs, RASs or automated switching systems that operate BES elements and either are presently in service or expected to be in service within the next 12-24 months.
- SPS, RASs or Automated Switching Systems Identification: Determine whether any of the listed SPSs, RASs or automated switching systems would cause one or more IROL violations for failure to operate as designed, or cause a reduction in one or more IROLs, if destroyed, degraded, misused, or otherwise rendered unavailable. Identify and list the applicable systems. For systems that have elements at multiple substation locations, identify and list the substations, which contain a portion of the applicable system that would cause one or more IROL violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the applicable SPSs, RASs or automated switching systems. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.

- Cyber System Identification: Update the list of BES Cyber Systems that are classified as Medium Impact Facilities.

Suggested Critical Evidence for Criterion 2.9:

1. Generator Owner and Transmission Owner - Lists of SPSs, RASs or automated switching systems, or portions of these systems that were determined to cause to one or more IROL violations for failure to operate as designed, or cause a reduction in one or more IROLs, if destroyed, degraded, misused, or otherwise rendered unavailable.
2. Generator Owner and Transmission Owner - Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.9.

Suggested Supporting Evidence for Criterion 2.9:

1. Generator Owner and Transmission Owner - Lists of Registered Entity-owned SPSs, RASs or automated switching systems that operate BES elements as supporting evidence.
2. Generator Owner and Transmission Owner - Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the list of applicable SPSs, RASs or automated switching systems as supporting evidence.

Criterion 2.10 *Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.*

Applicability: Distribution Providers and Transmission Owners that own UVLS systems or UFLS systems

- List of UVLS or UFLS Systems: Consideration should be given to those UFLS or UVLS that must be manually armed with automatic operation by a common system. Update a list of all Registered Entity-owned systems or group of Elements that perform automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing UVLS or UFLS under a load shedding program that are either presently in service or will be in service within the next 12-24 months.

  (For example: Where an entity owns 300MW of UFLS, that is controlled with individual UFLS relays (none of which can shed over 300 MW by itself), the UFLS relays themselves would not be considered Medium Impact Cyber Systems (unless they are under common control).

- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation,

identify and list the Cyber Assets used to perform one or more BES reliability operating services for the identified UVLSs or UFLSs. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, and Inter-Entity Coordination.

- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.10.

Suggested Critical Evidence for Criterion 2.10:

1. Lists of UVLSs or UFLS that meet Criterion 2.10.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.10.

Suggested Supporting Evidence for Criterion 2.10:

1. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with the applicable UVLSs or UFLSs as supporting evidence.

Criterion 2.11 *Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.*

Applicability: Generator Operators that own Controls Centers or backup Control Centers

- List of candidate Control Centers or backup Control Centers: Update a list of all Registered Entity-owned Controls Centers or backup Control Centers not already included in High Impact Rating (H) above that are presently in service.
- Control Center or Backup Control Center Identification: Determine which Controls Centers or backup Control Centers are used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a Eastern, Western, or ERCOT Interconnection and update a list of Controls Centers or backup Control Centers that meet this criterion.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the identified Control Centers or backup Control Centers. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Managing Constraints, Monitoring and Control, Restoration, Situation Awareness, and Inter-Entity Coordination.

- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.11.

Suggested Critical Evidence for Criterion 2.11:

1. Lists of applicable Controls Centers or backup Control Centers.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.11.

Suggested Supporting Evidence for Criterion 2.11:

1. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with applicable Control Centers or backup Control Centers as supporting evidence.

Criterion 2.12 *Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.*

Applicability: Transmission Operator that own Controls Centers or backup Control Centers

- List of candidate Control Centers or backup Control Centers: Update a list of all Registered Entity-owned Controls Centers or backup Control Centers not already included in High Impact Rating (H) above that either are presently in service or expected to be in service within the next 12 months.
- Control Center or Backup Control Center Identification: Determine which Controls Centers or backup Control Centers are used to perform the functional obligations of the Transmission Operator and update a list of Controls Centers or backup Control Centers that meet this criterion.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the identified Control Centers or backup Control Centers. These services are Dynamic Response, Balancing Load & Generation, Controlling Voltage, Managing Constraints, Monitoring and Control, Restoration, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.12.

Suggested Critical Evidence for Criterion 2.12:

1. Lists of applicable Controls Centers or backup Control Centers.
2. Lists of BES Cyber Systems that have a Medium Impact Ratings due to Criterion 2.12.

Suggested Supporting Evidence for Criterion 2.12:

1. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with applicable Control Centers or backup Control Centers as supporting evidence.

Criterion 2.13 *Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.*

Applicability: Owners of Control Centers or backup Control Centers that provide the Balancing Authority functional obligations

- List of candidate Control Centers or backup Control Centers: Update a list of all Registered Entity-owned Controls Centers or backup Control Centers not already included in High Impact Rating (H) above that either are presently in service or expected to be in service within the next 12 months.
- Control Center or Backup Control Center Identification: Determine which Controls Centers or backup Control Centers are used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in an Eastern, Western, or ERCOT Interconnection and update a list of Controls Centers or backup Control Centers that meet this criterion.
- Cyber Asset Identification: Identify and list the candidate Cyber Assets. Document the rationale used to determine the scope of candidate Cyber Assets. Consider the adverse impact that could occur within 15 minutes of loss, compromise, or misuse of the candidate Cyber Assets. If using the optional concept of BROS as criteria during the evaluation, identify and list the Cyber Assets that are used to perform one or more BES reliability operating services for the identified Control Centers or backup Control Centers. These services are Dynamic Response, Balancing Load & Generation, Controlling Frequency, Situation Awareness, and Inter-Entity Coordination.
- Cyber System Identification: Update the list of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.13.

Suggested Critical Evidence for Criterion 2.13:

1. Lists of applicable Controls Centers or backup Control Centers.
2. Lists of BES Cyber Systems that have Medium Impact Ratings based on Criterion 2.13.

Suggested Supporting Evidence for Criterion 2.13:

1. Lists of candidate Cyber Assets and identified BES Cyber Assets associated with applicable Control Centers or backup Control Centers as supporting evidence.

Evaluating CIP-002-5.1, Requirement R1.3

R1.3. *Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).*

CIP-002-5.1 - Attachment 1

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

Recommended Application Guidance:

Annually assign a Low Impact Rating to BES Cyber Systems that are not included in Sections 1 or 2 above and are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of the CIP-002-5.1 standard:

Suggested Critical Evidence for Criterion 3.1 – 3.6:

1. Lists of applicable assets.
2. Lists of BES Cyber Systems that have Low Impact Ratings.

Suggested Supporting Evidence for Criterion 3.1 – 3.6:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Criterion 3.1 *Control Centers and backup Control Centers.*

Applicability: Control Center and backup Control Center owners

- Update list of BES control centers or backup control centers control centers and backup control centers that are not already included in the identification of a High or Medium Impact Rating, are Registered Entity-owned, and are presently in service or expected to be in service within 12 months.
- Annually determine which BES Cyber Systems are located at BES control centers or backup control centers that did not qualify under the High or Medium Impact criterion.
- Annually update the list of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.1.

Suggested Critical Evidence for Criterion 3.1:

1. Lists of applicable Controls Centers or backup Control Centers.
2. Lists of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.1.

Suggested Supporting Evidence for Criterion 3.1:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Criterion 3.2 *Transmission stations and substations.*

Applicability: Transmission Owners

- Update its list of BES transmission stations and substations that are not already included in the identification of a High or Medium Impact Rating, are Registered Entity-owned, and are presently in service or expected to be in service within 12 months.
- Annually determine which BES Cyber System(s) are located at BES transmission stations and substations that did not qualify under the High or Medium Impact criterion.
- Annually update the list of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.2.

Suggested Critical Evidence for Criterion 3.2:

1. Lists of applicable Transmission stations and substations.

Lists of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.2.

Suggested Supporting Evidence for Criterion 3.2:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Criterion 3.3 *Generation resources.*

Applicability: Generation Owners

- Update its list of generation resources that are not already included in the identification of a High or Medium Impact Rating, are Registered Entity-owned, and are presently in service or expected to be in service within 12 months.
- Annually determine which BES Cyber System(s) are located at BES generation resources that did not qualify under the High or Medium Impact criterion.
- Annually update the list of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.3.

Suggested Critical Evidence for Criterion 3.3:

1. Lists of applicable Generation resources.
2. Lists of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.3.

Suggested Supporting Evidence for Criterion 3.3:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Criterion 3.4 *Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.*

Applicability: Registered Entities that own *Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.*

- Update its list of BES systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements that are Registered Entity-owned, and are presently in service or expected to be in service within 12 months.
- Annually determine which BES Cyber System(s) are located at BES assets containing systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements, that did not qualify under the High or Medium Impact criterion.
- Annually update the list of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.4.

Suggested Critical Evidence for Criterion 3.4:

1. Lists of applicable systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
2. Lists of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.4.

Suggested Supporting Evidence for Criterion 3.4:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Criterion 3.5 *Special Protection Systems that support the reliable operation of the Bulk Electric System.*

Applicability: Registered Entities that own SPSs, RASs or automated switching systems that operate BES elements.

- Update its list of BES special protection systems that are not already included in the identification of a High or Medium Impact Rating, are Registered Entity-owned, and are presently in service or expected to be in service within 12 months.
- Annually determine which BES Cyber System(s) are located at BES assets containing Special Protection Systems that did not qualify under the High or Medium Impact criterion.
- Annually update the list of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.4.

Suggested Critical Evidence for Criterion 3.5:

1. Lists of applicable Special Protection Systems.
2. Lists of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.5.

Suggested Supporting Evidence for Criterion 3.5:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Criterion 3.6 *For Distribution Providers, Protection Systems specified in Applicability section 4.2.1*

> ***Applicability 4.2.1.*** *Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:*
>
> ***4.2.1.1.*** *Each UFLS or UVLS System that:*
>
> ***4.2.1.1.1.*** *is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and*
>
> ***4.2.1.1.2.*** *performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.*
>
> ***4.2.1.2.*** *Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.*
>
> ***4.2.1.3.*** *Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.*
>
> ***4.2.1.4.*** *Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.*

Applicability: *Distribution Providers that own Protection Systems specified in Applicability section 4.2.1 above*

- Update its list of BES protection systems that meet Applicability 4.2 and are not already included in the identification of a High or Medium Impact Rating, are Registered Entity-owned.
- Annually determine which BES Cyber System(s) are located at BES assets containing BES Protection Systems that did not qualify under the High or Medium Impact criterion.
- Annually update the list of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.6.

Suggested Critical Evidence for Criterion 3.6:

1. Lists of applicable Registered Entity-owned Distribution Provider Protection Systems.
2. Lists of BES Cyber Systems that have Low Impact Ratings based on Criterion 3.6.

Suggested Supporting Evidence for Criterion 3.6:

1. Lists of candidate assets and those not identified as BES assets as supporting evidence.

Evaluating CIP-002-5.1, Requirement 2

CIP-002-5.1 Requirement 2 defines the required periodicity and approvals for the execution of Requirement 1.

> ***R2:*** *The Responsible Entity shall: [Violation Risk Factor: Lower][Time Horizon: Operations Planning]*
>
> ***2.1*** *Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and*
>
> ***2.2*** *Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.*

Analysis:

- The periodicity allowed in the standard is every 15 months. However, a periodicity of once during the timeframe between January 1 and December 31 of each consecutive year without exceeding 15 months between the performance of tasks, is suggested. Establishing a schedule where planned activities occur on a specific date each year (or at the same time every year), not to exceed 15 calendar months, is the recommended approach for the review of the CIP-002-5.1 processes and documentation to validate that the previous assessments remain accurate. A cycle to perform these tasks at the same time every year may be easier to set up, remember, and coordinate with routine transmission system planning and records updating that occurs on a similar cycle. Retention of required and supporting documentation on a basis of once per calendar year would be easier to organize and retrieve.
- The annual review and update process described in Requirement part 2.2 should be a team effort to include operational subject matter experts representing the assets that were inventoried for analysis. Within this annual process, it is important to capture new assets (within the Operations Planning Time Horizon) and analyze them for the appropriate impact levels, and to de-list assets that have been retired or otherwise removed from scope.

Tip:

1. If the Impact Ratings list is null, then clearly document that the list is null.
2. Include the names of the preparer and approver, as well as the date on all critical and supporting evidence documents.

Suggested Critical Evidence for R2:

All lists developed for Requirement 1, including the supporting supplemental materials used to develop the lists, should be made available to the CIP Senior Manager as basis for his/her review and approval. Additionally, these materials should be retained per the Registered Entity's document retention policies.

Evidence that the approval(s) occurred on a specific date should be maintained. Evidence can be system-generated (electronic) in the form of time-stamps from a document management system or workflow tool, dated meeting minutes, or email calendar invitations. It can also be physical pen & ink signatures on paper, with a primary and secondary copy stored in separate locations. Registered Entities may want to consider scanning and retaining an electronic copy of paper records with pen & ink signatures.

Suggested Supporting Evidence for R2:

If the review for Requirement part 2.2 is to be performed by a delegate, ensure that a copy of that delegation agreement is available, current, and in-force at the time of the annual approval. Keep a copy of the delegation agreement with the other evidence requirement by Requirements R1 and R2.

MITIGATING RISK AND INTERNAL CONTROLS

As with any internal control, only the Registered Entity can determine the depth and breadth of its controls. Internal Controls should be in place for entity determined "high" risk items, so the entity can reasonably assure there is no "drift" of the entity's stated expectations of its system operators. Registered Entities are encouraged to design and implement the concept of self-monitoring for internal controls as a part of continuous improvement and Corrective Action Programs.

Management Practices (Internal Controls)

1. Lists associated with each criterion should be reviewed and approved by the manager, or managers, associated with each criterion evaluation.
2. Interpretations or rationales associated with each criterion should be formally documented and include the preparer's name, creation date, and approver's name.
3. The CIP Senior Manager or delegate should review all supplemental lists that were used to develop the lists required in Requirement R1, to ensure the conclusions were reasonable.
4. Review any delegation agreements created per CIP-003-5 Requirement R4 to ensure the delegation is current, approved, and in-force prior to any delegate approving the lists required for CIP-002-5.1.
5. Periodic spot checks of the Cyber Asset inventory for BES asset facilities.
6. Administrative controls or triggers to identify mid-cycle changes and corresponding processes to allow for mid-cycle updates of documentation.
7. Training program that enables subject-matter experts to stay proficient on CIP-002-5.1 concepts and to ensure that design/engineering for new BES asset facilities is compatible with the cyber security requirements of the CIP reliability standards.

APPENDIX A: REFERENCES

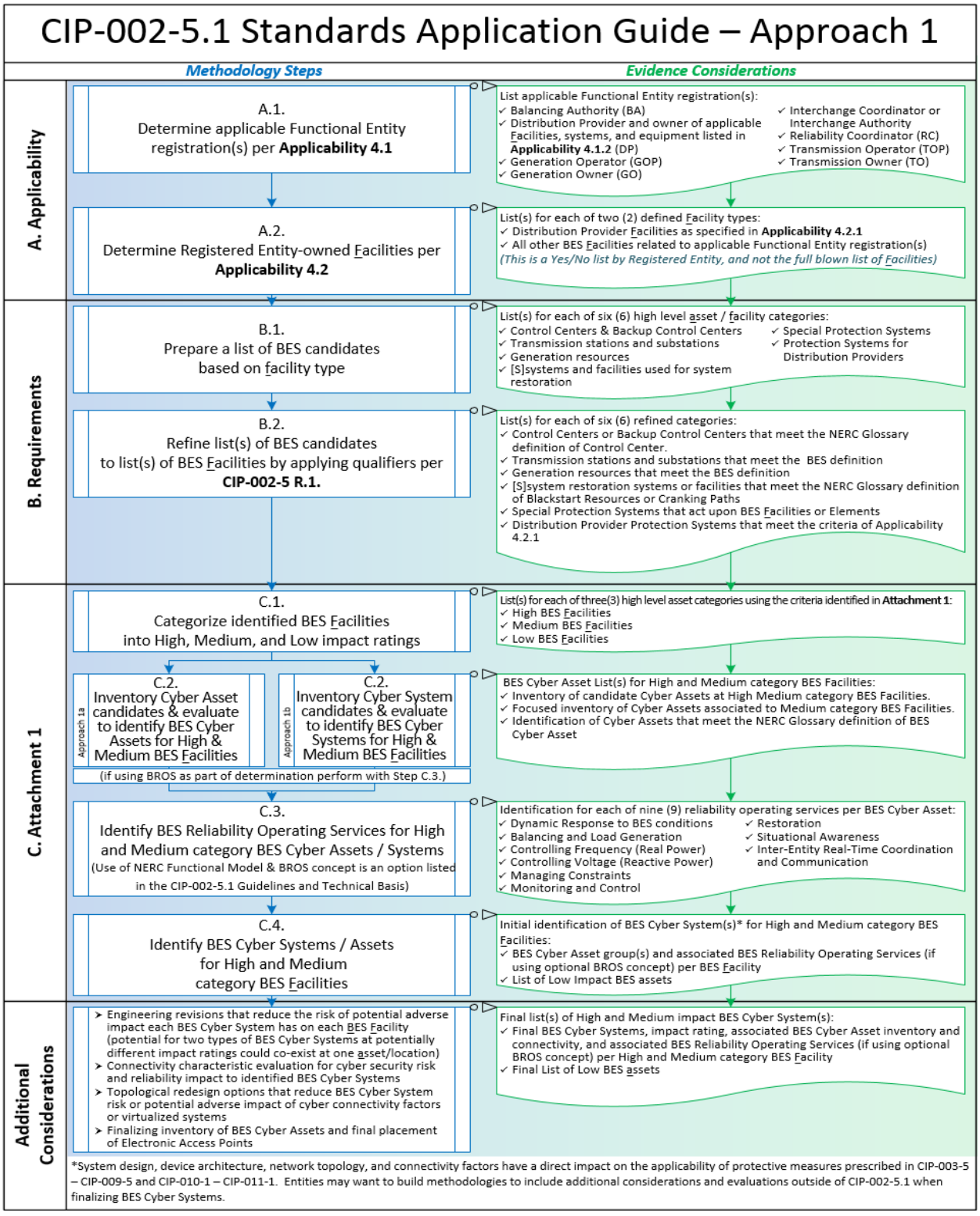
1. NERC Reliability Standard CIP-002-5.1 (Cyber Security — BES Cyber System Categorization). Retrieved from: http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization&jurisdiction=null
2. NERC Glossary of Terms. Retrieved from: http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf
3. NERC Functional Model. Retrieved from: http://www.nerc.com/pa/stand/pages/functionalmodel.aspx

APPENDIX B: COMPANION DOCUMENTS

This is a list of supplemental documents which are provided as attachments in the left hand column of this PDF document when downloaded and opened in Adobe Acrobat. If you're interested in obtaining a copy of one of these documents and are unable to open in Adobe Acrobat, please email the CIP SME team by clicking here.

Description	Filename(s)
Substation logical diagrams, identifying BCS	Substation_diagram.pdf
Generation logical diagrams, identifying BCS	Generation_diagram.pdf
Control Center logical diagrams, identifying BCS	ControlCenter_diagram.pdf
Standard Application Workbook Forms	Attachment1_Worksheets.docx
Cyber Asset assessment methodology and procedure • Associated data worksheets for Cyber Asset inventory and scoping are attachments within the CyberAssetProcedure.pdf document	Cyber_Asset_Procedure.docx • High_impact.xlsx Medium_impact.xlsx • Low_impact.xlsx • PACS.xlsx • EACMS.xlsx • EAP
High & Medium Impact Cyber Asset Connectivity Scenarios and applicable protective measures	Cyber Asset Classifications and ESP-PSP requirements.vsd
General implementation considerations	Implementation.docx

APPENDIX C: RECOMMENDED APPROACH



APPENDIX D: TOP-DOWN VARIATIONS

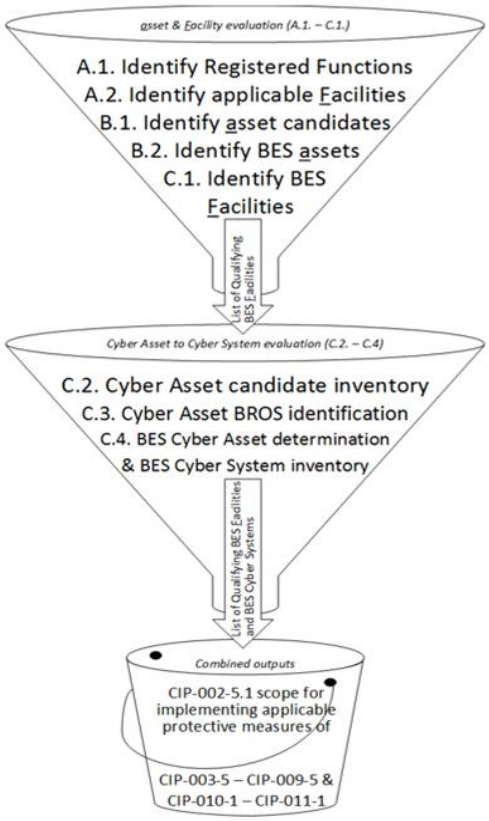
Cyber Asset-based candidate method

Approach 1.a. is a top-down method that may be most practical for assets:

- where the majority of Cyber Assets and systems are dedicated to and pertinent to BES operation,
- where the Cyber Assets are within (or mostly within) a single logical security zone/trust level at the asset,
- where an asset-wide, or full, Cyber Asset inventory is the most judicious means to achieve a comprehensive Cyber Asset candidate inventory, or
- where an asset-wide Cyber Asset inventory is less/equally burdensome as alternative means to identify Cyber Assets candidates at the asset, or
- an alternative mechanism to achieve a comprehensive Cyber Asset candidate inventory does not exist for the asset

Entities may want to consider this approach as illustrated below for an asset that is dedicated (or mostly dedicated) to a single function.

Examples: Smaller unmanned generation facilities, or transmission stations or substations



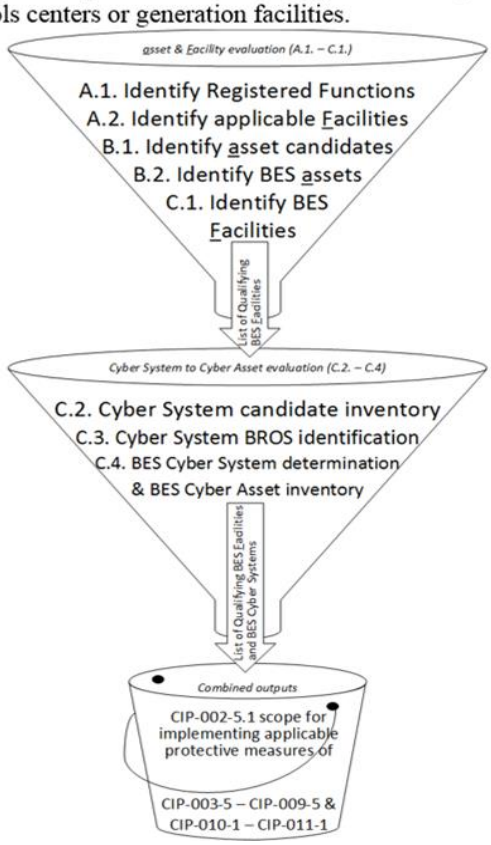
Cyber System-based candidate method

Approach 1.b. is another top-down method that may be more practical for assets:

- that contain volumes of Cyber Assets and systems not pertinent to BES operation,
- where several logical security zones/trust levels exist between Cyber Assets at the asset,
- where a comprehensive inventory could be achieved via alternative mechanisms like, but not limited to, analysis of access capability at points of ingress/egress between logical security zones/trust levels to identify Cyber Asset candidates outside of a logical environment that is pertinent to BES operation, and
- where an asset-wide Cyber Asset inventory is inefficient and/or burdensome compared to alternative Cyber Asset candidate inventory identification methods

Entities may want to consider this alternative approach as illustrated below for an asset that contains more than one function beyond BES reliability operating services

Example: Large facilities with multiple functions, like controls centers or generation facilities.



REVISIONS

February 18, 2015

- ***Cyber_Asset_Procedure.docx***:
  - Formula driven sample workbooks have been created and attached to this companion document to assist entities in applying the methodology outlined in the sample procedure
  - Several of the detailed flow diagrams within the appendices of the procedure have been updated to align with the accompanying workbooks
  - An additional flow diagram and workbook have been added to supplement the example process flow for identifying Electronic Access Points

- ***Cyber_Asset_Classifications_and_ESP-PSP_requirements.pdf***:
  - The intention of this companion document was to depict the relationship between Electronic Security and Physical Security requirements for CIP-005-5 and CIP-006-5 to various topologies, cyber configurations, or redesign options for BCSs identified in CIP-002-5.1
  - The diagram originally depicted both High and Medium impact scenarios as a single illustration
    - This has been split out into two separate diagrams to provide clarity about the differences between High impact and Medium impact BCSs as it relates to applicability and connectivity factors outside of CIP-002-5.1