I. PROCEDURE SUMMARY

- This procedure provides the Site with written guidance to maintain compliance with Reliability Standard CIP-002. The Standard requires a periodic evaluation of BES Cyber Systems and their impact rating to ensure correct categorization.
- Applicability: GO, GOP
    - All BES Cyber Systems under Site are subject to the requirements of this procedure.
    - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters are exempt from the requirements of this procedure.
- **The effective date of the procedure is based off the Asset Management Approval date.

REVISION INDEX

Revision	Section Revised	Comments	Effective Date
rev00	All	Initial Release	

II. TABLE OF CONTENTS

III. DETAILED PROCEDURE

1.0 PURPOSE

The purpose of this procedure is to identify and categorize Bulk Electric System (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.

- For site-specific information (which is italicized and underlined), refer to the Site Data Sheet. Section 7.0 and attachment(s) will not refer to the CIP Site Data Sheet. All specific site information needed will have been identified in previous sections.

2.0 REFERENCES

2.1 NERC Standard CIP-002-5.1a, "Cyber Security – BES Cyber System Categorization"

2.2 Standard Application Guide CIP-002-5.1, *Midwest Reliability Organization* Standards Committee, January 8, 2015.

2.3 Cyber Asset Matrix (or similar document)

2.4 BHER-PRO-CIP-003, "Security Management Controls"

3.0 DEFINITIONS

Capitalized terms used herein and not defined herein shall have the meanings as described to such terms in the NERC "Glossary of Terms used in NERC Reliability Standards" located at http//www.nerc.com

3.1 **"Adverse Reliability Impact"** – The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.

3.2 **"BES Cyber Asset (BCA**)" – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

3.3 **"BES Cyber System (BCS)"** – One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

3.4 **"Blackstart Resource"** – A generating unit(s) and its associated set of equipment which has the ability to be started without support from the system or is designed to remain energized without connection to the remainder of the system, with the ability to energize a bus, meeting the *Transmission Operator's* restoration plan needs for Real and Reactive Power capability, frequency and voltage control, and that has been included in the *Transmission Operator's* restoration plan.

3.5 **"Bulk Electric System (BES)"** – See NERC "Glossary of Terms Used in NERC Reliability Standards" definition.

3.6 **"Bulk-Power System – Bulk Power System"** - (A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. (Note that the terms "Bulk-Power System" or "Bulk Power System" shall have the same meaning.)

3.7 **"Cascading"** – The uncontrolled successive loss of System Elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.

3.8 **"*CIP Senior Manager*"** – A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.

3.9 **"Contingency"** – The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element.

3.10 **"Control Center"** – One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a *Reliability Coordinator*, 2) a *Balancing Authority,* 3) a *Transmission Operator* for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

3.11 **"Cranking Path"** – A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units.

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

3.13 **"Element"** – Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An Element may be comprised of one or more components.

3.14 **"Equipment Rating"** – The maximum and minimum voltage, current, frequency, real and reactive power flows on individual equipment under steady state, short-circuit and transient conditions, as permitted or assigned by the equipment owner.

3.15 **"Facility"** – 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.)

3.16 **"Facility Rating"** – The maximum or minimum voltage, current, frequency, or real or reactive power flow through a facility that does not violate the applicable equipment rating of any equipment comprising the facility.

3.17 **"Interconnection"** – A geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control. When capitalized, any one of the four major electric system networks in North America: Eastern, Western, ERCOT and Quebec.

3.18 **"Interconnection Reliability Operating Limit (IROL)"** – A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System.

3.19 **"Load"** – An end-use device or customer that receives power from the electric system.

3.20 **"Reactive Power"** – The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive Power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive Power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).

3.21 **"Real Power"** – The portion of electricity that supplies energy to the Load.

3.22 **"Reliable Operation"** – Operating the elements of the [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

3.23 **"Special Protection Systems (SPS) / Remedial Action Scheme (RAS)"** – See NERC "Glossary of Terms Used in NERC Reliability Standards" definition.

3.24 **"System"** – A combination of generation, transmission, and distribution components.

3.25 **"System Operating Limit"** – The value (such as MW, Mvar, amperes, frequency or volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable

reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to:

- Facility Ratings (applicable pre- and post-Contingency Equipment Ratings or Facility Ratings)
- transient stability ratings (applicable pre- and post-Contingency stability limits)
- voltage stability ratings (applicable pre- and post-Contingency voltage stability)
- system voltage limits (applicable pre- and post-Contingency voltage limits)

4.0 RESPONSIBILITIES

4.1 The Site shall ensure a process is implemented to identify and categorize the *Impact Rating* Level for each BES Cyber System and their associated BES Cyber Assets.

4.2 The Site will review and update the BES Cyber Security Categorization procedure as required.

4.3 The Site shall:

4.3.1 Review the BES Cyber Systems *impact rating* level identifications in Requirement R1 at least yearly, not to exceed once every 15 calendar months.

4.3.2 Update the categorization of the BES Cyber System and associated BES Cyber Assets if identifications have changed.

4.3.3 The Site's *CIP Senior Manager*, or their delegate, shall approve the CIP *Impact Rating* identification review yearly, not to exceed once every 15 calendar months.

5.0 DETAILS

5.1 The Site shall implement a process that considers the following for the purpose of identifying the BES Cyber System Impact level. Identification of BES Cyber Systems may be accomplished using any of the methodologies provided in Attachment 2, "Identification of BES Cyber Systems:"

5.1.1 Control Centers and backup Control Centers

5.1.2 Transmission stations and substations

5.1.3 Generation resources

5.1.4 Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements

5.1.5 Special Protection Systems that support the reliable operation of the Bulk Electric System

5.1.6 For Distribution Providers, Protection Systems specified in NERC Standard CIP-002 section 4.2.1.

5.2 The Site shall evaluate the BES Cyber Systems and their associated BES Cyber Assets identified in 5.1 above against the criteria listed in Attachment 1, "Impact Rating Criteria" and:

5.2.1.1 Identify each *high impact* BES Cyber System at the asset, if any

5.2.1.2 Identify each *medium impact* BES Cyber System at the asset, if any

5.2.1.3 Identify each asset that contains a *low impact* BES Cyber System

5.2.2 The Site shall review the identifications of the Impact Evaluation and associated BES Cyber Assets yearly, not to exceed 15 calendar months.

5.2.3 The Site shall update the BES Cyber System categorization(s) if any changes are identified.

5.2.4 The Site's *CIP Senior Manager*, or their delegate, shall approve the identifications, not to exceed 15 calendar months.

5.2.5 The Site's shall also evaluate the identified BES Cyber System, and their associated BES Cyber Assets, against the criteria listed in Attachment 1, "Impact Rating Criteria". Evidence from the from the Applicable *Planning Coordinator* and/or Applicable *Transmission Planner* and/or Applicable *Reliability Coordinator* will be required to demonstrate that each required criterion is or is not applicable.

5.2.5.1 For Attachment 1 criterion 2.3, The Site shall verify with Applicable *Planning Coordinator* or Applicable *Transmission Planner* that this criterion is not met by the asset(s) associated with the BES Cyber System being evaluated.

5.2.5.2 For Attachment 1 criterion 2.6, The Site shall verify with Applicable *Reliability Coordinator*, Applicable *Planning Coordinator*, or Applicable *Transmission Planner* that this criterion is not met by the asset(s) associated with the BES Cyber System being evaluated.

5.2.5.3 For Attachment 1 criterion 2.9, for each applicable *Remedial Action Scheme (RAS),* The Site shall verify with Applicable *Reliability Coordinator*, Applicable *Planning Coordinator*, or Applicable *Transmission Planner* that this criterion is not met by any *RAS* associated with the BES Cyber System being evaluated.

5.2.6 If the *impact rating* for any of The Site's BES Cyber Systems has changed, the *CIP Senior Manager*, or their delegate, shall initiate additional actions, if any, to comply with the relevant CIP Standards and Requirements for the new *impact rating*.

5.3 The Site shall update all related documentation (e.g., diagrams, lists, etc.) as necessary (Ref. *Cyber Asset Matrix*).

6.0 RECORDS

6.1 The Site shall ensure appropriate reports, data sheets, spreadsheets, specifications, emails, letters, procedures, logs, compliance records, memoranda, or other dated documentation are retained as evidence of compliance for a minimum period equal to the longest of the following:

- 3 calendar years;
- The full time period since the end of the last audited period;
- For specific evidence that is related to a compliance violation, the period until mitigation is complete and approved by the Compliance Enforcement Authority; or
- For specific evidence that is part of any other investigation, the period specified by the Compliance Enforcement Authority.

6.2 The Site shall keep the last audit records and all requested and submitted subsequent audit records.

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

7.1 (CIP-002 R1) Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

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 operation of the Bulk Electric System; and

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.

7.1.1 (1.1) Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

7.1.2 (1.2) Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset.

7.1.3 (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).

7.2 (CIP-002 R2) The responsible Entity shall:

7.2.1 (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

7.2.2 (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.

7.3 Impact Evaluation

8.0 ATTACHMENTS

8.1 Attachment 1: Impact Rating Criteria

8.2 Attachment 2: Identification of BES Cyber Systems

ATTACHMENT 1
Impact Rating Criteria

CIP-002-5.1a - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

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

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

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.

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.

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.

2. Medium Impact Rating (M)

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

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.

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.

ATTACHMENT 1
Impact Rating Criteria

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.

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.

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

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.

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

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.

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.

ATTACHMENT 1 **Page 3 of 4**
Impact Rating Criteria

ATTACHMENT 1
Impact Rating Criteria

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.

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.

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.

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.

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:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

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

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

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

ATTACHMENT 2 **Page 1 of 9**
Identification of BES Cyber Systems

General Information

Purpose

The purpose of this Attachment is to provide guidance on how to identify BES Cyber Systems that would be subject to the categorization process required by NERC Standard CIP-002.

References

For references made by this guidance document to other documents, refer to the References section in the main body of this procedure.

Definitions

For definitions of the terms used and referenced in this guidance document, refer to the Definitions section in the main body of this procedure.

Contents

This guidance document contains information regarding the following methods for identifying BES Cyber Systems, discussed in detail in the sections below. This guidance document is not intended to be all-inclusive. Other methods or variations of the described methods may be used at the discretion of the CIP Senior Manager.

- BES Reliability Operating Service (BROS)
- Top-down Approach
- Bottom-up Approach

BES Reliability Operating Service (BROS)

This methodology is described in NERC Standard CIP-002-5.1a and relies on first identifying the services associated with registered functions and then the systems that accomplish those services. The below information is taken directly from the Guidelines and Technical Basis.

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “...that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES

ATTACHMENT 2 **Page 2 of 9**
Identification of BES Cyber Systems

Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity Coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that maybe considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO, GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO, TOP, GO, GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)

- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO, DP)

- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP, TO, DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO, DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flowgates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

ATTACHMENT 2 **Page 6 of 9**
Identification of BES Cyber Systems

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC, BA)
- Change management (TOP, GOP, RC, BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA, TOP, GOP, RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Top-down Approach

The “top-down” approach is also known as the “facility-centric” approach. This methodology is so named because it begins with first identifying and categorizing owned facilities (think of “facilities” as ‘locations of’ or ‘containers for’ equipment and systems that support the BES, and not the NERC-defined term, “Facilities”) and then moves on to identifying the associated BES Cyber Systems and BES Cyber Assets. The methodology description that follows is a simplified version of “Standard Application Guide CIP-002-5.1,” published by the Midwest Reliability Organization Standards Committee, available on the NERC website.

The first step is to determine applicability per the Applicability section of NERC Standard CIP-002, which has multiple parts. Determine the following:

1. Am I a functional entity listed under NERC Standard CIP-002, section 4.1? If yes, document your entity’s registered functions.

2. Do I own any Facilities (note that this is referring to the NERC-defined term) listed under NERC Standard CIP-002, section 4.2? If yes, document the asset types your registered entity owns.

3. If the answer is yes to both questions, CIP-002 is applicable, and your registered entity is subject to its requirements.

Once applicability has been established, it is appropriate to consider the Requirements of NERC Standard CIP-002.

1. Refer to the list of BES assets given in Requirement R1, i-vi. If your registered entity owns assets of these types, a list of those assets should be documented for further evaluation. An asset may either be a facility (i.e., location) or a Facility (as defined by NERC).

2. Verify that the listed assets meet the following criteria for their asset types, removing those that do not meet the threshold.

    - For Control Centers and backup Control Centers, the NERC Glossary of Terms definition of “Control Center;”

    - For Transmission stations and substations, the NERC Glossary of Terms definition of “Bulk Electric System;”

    - For Generation resources, the NERC Glossary of Terms definition of “Bulk Electric System;”

    - For systems and facilities critical to system restoration, the NERC Glossary of Terms definitions of “Blackstart Resource” and “Cranking Path.”

    - For Special Protection Systems, these systems must support the reliable operation of the Bulk Electric System.

    - If at least one of your registered functions is as a Distribution Provider, for Protection Systems, these systems must meet the criteria of NERC Standard CIP-002, section 4.2.1.

    It is important to establish the applicability of these assets with respect to their NERC definitions, as the defined assets have an implicit or explicit area of influence that couples with the Impact Rating Criteria. For example, generation resources have a control room, but the control room is not recognized under CIP-002 (or any other NERC Standard) as a Control Center if it does not control generation at two or more locations. In this example, a control room that has control over a single, local generation resource will not have as large an area of influence as a Control Center that controls generation

resources at multiple locations; hence, there is potential for a higher impact rating for the Control Center.

After a list of applicable assets is finalized, they can be evaluated against the associated Impact Rating Criteria from NERC Standard CIP-002 Attachment 1. Note that it is not the intent of the Standard to identify an impact rating for an asset and then associate all BES Cyber Systems contained within this asset with the same rating, as assets may be comprised of several BES Cyber Systems and, conversely, a single BES Cyber System may span across multiple assets. Determining the impact that an asset has to the Bulk Electric System is an intermediate step in determining BES Cyber System impact.

1. For Control Centers and backup Control Centers, high impact criteria 1.1 – 1.4 and medium impact criteria 2.11 – 2.13 apply;

2. For Transmission stations and substations, medium impact criteria 2.1 – 2.10 apply;

3. For Generation resources, medium impact criteria 2.1 – 2.10 apply.

4. For any assets that did not meet any of the high or medium impact criteria, these are considered to have low impact.

With applicable assets categorized, the next step is to inventory the BES Cyber Assets associated with your registered entity's listed assets. The inventory is required for assets that are captured in the high and medium Impact Rating Criteria to ensure that any and all high and medium impact BES Cyber Systems are identified. An inventory, or discrete list, of BES Cyber Assets is NOT required for any remaining assets whose BES Cyber Systems would automatically be categorized as low impact; however, it is strongly recommended that these be identified to aid in the application of security controls.

1. For each categorized asset, create a list of devices located at the asset.

2. From the device list, identify those devices that support the asset's reliability function. It may be helpful to refer to the BROS functions to identify those functions that are related to reliability. The identified devices may include devices that support communication pathways between other key devices.

3. Using the NERC Glossary of Terms definition, determine which of those devices are Cyber Assets

4. Using the NERC Glossary of Terms definition, determine which of those Cyber Assets meet the threshold for being identified as BES Cyber Assets.

5. For all BES Cyber Assets identified, identify logical groupings of the BES Cyber Assets. This may fall along the lines of the overall function they achieve together, the way they are physically connected, or both. These groups are considered BES Cyber Systems.

ATTACHMENT 2 **Page 9 of 9**
Identification of BES Cyber Systems

Bottom-up Approach

The “bottom-up” approach is also known as the “system-centric” approach. This methodology is so named because it begins with first inventorying the population of all BES Cyber Assets and BES Cyber Systems before attributing them to BES assets (or “facilities,” not to be confused with the NERC-defined term, “Facilities”). Because identification criteria/thresholds are the same as in the Top-down Approach, only a summary of the re-ordered steps is provided below.

1. Inventory of Cyber Assets

   Create a list of devices and determine whether they are Cyber Assets, whether they are related to any reliability functions, and identify those that meet the definition of BES Cyber Assets. Then group these Cyber Assets into BES Cyber Systems.

2. Applicability

   Verify that your registered entity falls under at least one of the registered functions for which CIP-002 applies. Note that some registered functions may have additional applicability criteria.

3. CIP-002 R1 Asset List

   Determine whether your registered entity owns any of the asset types listed in CIP-002 Requirement R1. Verify these identifications according to NERC definitions and the criteria described within CIP-002.

4. Impact Rating Criteria

   Review the Impact Rating Criteria in CIP-002 Attachment 1 for each of the identified asset types. Associate the BES Cyber Systems that were previously identified with the assets and functions delineated by the Impact Rating Criteria.