MIDWEST RELIABILITY ORGANIZATION
380 St. Peter Street, Suite 800, Saint Paul, MN 55102 MidwestReliability.org P. 651.855.1760 F. 651.855.1712

[Registered Entity Name]

NERC ID: [NCRXXXXX]

CIP-002-5.1 - Cyber Security – BES Cyber System Categorization

2nd Quarter 2016 Guided Self-Certification (Revised)

380 St. Peter Street, Suite 800, Saint Paul, MN 55102 MidwestReliability.org P. 651.855.1760 F. 651.855.1712

Instructions

1. Populate the cover page by adding your entity's name and NERC identification number.
2. Complete the tasks listed under **Assessment Guidance**.
3. Log into **webCDMS** and complete your self-certification response.
4. Submit via the MRO EFT Encrypted Site:
    a. This completed Worksheet; and
    b. Specific evidence requested within this document. Please make sure to use unique file names for each evidence file submitted, and identify within your narratives which specific evidence files support each conclusion made. These references and the use of unique file names helps facilitate and expedite MRO's review of the Guided Self-Certification work that has been performed.

Scope

CIP-002-5.1 - Cyber Security – BES Cyber System Categorization – R1

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. *Transmissions 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, Protections Systems specified in Applicability section 4.2.1.*

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;*

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).*

Applicability:

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.

CIP-002-5.1 - 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.

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.

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.

MIDWEST RELIABILITY ORGANIZATION
380 St. Peter Street, Suite 800, Saint Paul, MN 55102 MidwestReliability.org P. 651.855.1760 F. 651.855.1712

Assessment Guidance

NOTE: All wholly- and jointly-owned BES Assets and BES Cyber Systems must be accounted for when completing this Self-Certification. Ensure you list all owners of each BES Asset along with who operationally controls it. Due to the nature of jointly-owned BES Assets in the MRO region, this extra step is provided to ensure jointly-owned BES Assets are included. If you have additional questions about any joint-ownership items to include, contact the proper individual listed in the Self-Certification Notification Letter.

Part 1 – Response Due to MRO by July 15, 2016 (Previously April 30, 2016)

1. Using your list of BES Cyber Systems identified per R1, please complete the included worksheet, "ERO CIP V5 Self-Cert Worksheet.xls," and provide the completed worksheet to MRO. The purpose of the worksheet is to capture the number of BES Assets that contain High-, Medium-, and/or Low-Impact BES Cyber Systems and the Impact Rating Criteria from Attachment 1 from which the BES Cyber Systems' Impact Rating was derived.

   Within the worksheet, complete a row for each BES Asset or group of BES Assets of the same type, per the "Asset Type" column, that have the same combination of High-, Medium-, and Low-Impact BES Cyber Systems. For each group, include the number of BES Assets that comprise the group; a brief description of the group; whether the BES Assets in the group contain High-, Medium, and/or Low-Impact BES Cyber Systems; whether the BES Assets in the group are accessible via routable connectivity; and an indication of whether or not each of the Attachment 1 Impact Rating Criteria were satisfied by the BES Assets.

   For additional instructions for completion of each column within the worksheet, please see the worksheet's "Description of Headings" tab.

BES Asset Count/Categorization Spreadsheet	
Filename	
Comments	

Part 2 – Response Due to MRO by July 15, 2016 (Previously June 30, 2016)

1. Per Requirement R1, provide the document(s) that describes your process to identify BES Cyber Systems.

BES Cyber System Categorization Process Document	
Filename	
Comments	

2. Per Requirement R1, does your process to identify BES Cyber Systems consider each of the following assets types:

   i. Control Centers and backup Control Centers;
   ii. Transmissions 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, Protections Systems specified in Applicability section 4.2.1.

☐ Yes.
☐ No, respond "Not Compliant" for R1 to the Self-Certification in webCDMS.

3. Update your Facility verification form to include a list of all wholly-owned or jointly-owned BES Assets and all of the 'Operators' for said BES Assets. Ensure you update all of the tabs including 'Transmission Lines,' 'BES Substations,' 'TOP,' 'Generators,' and '3rd-Party Gen.'

NOTE: All wholly- and jointly-owned BES Assets must be accounted for. Ensure you list all owners of each BES Asset along with who operationally controls it. Due to the nature of jointly-owned BES Assets in the MRO region, this extra Step is provided to ensure jointly-owned BES Assets are included. If you have additional questions about any joint-ownership items to include, contact the proper individual listed in the Self-Certification Notification Letter.

Updated Facility Verification Form	
Filename	
Comments	

The latest Facility Verification sheet received by MRO was provided with your Self-Certification Questionnaire.

4. Per Requirement R1.1, provide your list of High Impact BES Cyber Systems, description of what each High Impact BES Cyber System contains (e.g. their function, types of operation(s) it performs, etc.), and the BES Asset where each High Impact BES Cyber System is located. Within the list also identify all the owners for each High Impact BES Cyber System along with who is responsible for meeting the associated compliance obligations. If you do not have any High Impact BES Cyber Systems, skip to step 7.

High Impact BES Cyber Systems	
Filename	
Comments	

5. Select a random sample from your population identified in step 4 using the following sampling logic. (A random sample can be selected using statistical functions available in Microsoft Excel or through use of RAT-STATS, a free sampling tool available from the U.S. Department of Health & Human Services Office of Inspector General.)

From the population:
a. Select at least 10% of the population (maximum number sampled 10) making sure at least five are sampled (e.g. if fewer than 50 exist in your population, select at least five).
b. If five or fewer total exist in the population, select the whole population.

Also provide supporting evidence of the sampling process used including: (1) full population, (2) samples selected, and (3) output from the statistical function used to perform the sampling (e.g. RAT-STATS output).

File(s) Contents	*File Name / Page(s)*
Full Population	
Samples Selected	
Statistical Function Output	
Comments	

6. Per Requirement R1.1, for each item selected in the sample from step 5 above, provide any existing documented analysis as to why the asset was categorized as a "High Impact Cyber System." Please also ensure that you include which criteria were met within Attachment 1.

High Impact Cyber System Analysis	
Filename	
Comments	

Was each sample selected in step 5 identified as a High Impact BES Cyber System according to Attachment 1, Section 1?

☐ Yes.
☐ No, respond "Not Compliant" for R1 to the Self-Certification in webCDMS.

7. Per Requirement R1.2, provide your list of Medium Impact BES Cyber Systems, description of what each Medium Impact BES Cyber System contains (e.g. their function, types of operation(s) it performs, etc.), and the BES Asset where each Medium Impact BES Cyber System is located. Within the list also identify all the owners for each Medium Impact BES Cyber System along with who is responsible for meeting the associated compliance obligations. If you do not have any Medium Impact BES Cyber Systems, skip to step 10.

Medium Impact BES Cyber Systems	
Filename	
Comments	

8. Select a random sample from your population identified in step 7 using the following sampling logic. (A random sample can be selected using statistical functions available in Microsoft Excel or through use of RAT-STATS, a free sampling tool available from the U.S. Department of Health & Human Services Office of Inspector General.)

From the population:

c. Select at least 10% of the population (maximum number sampled 10) making sure at least five are sampled (e.g. if fewer than 50 exist in your population, select at least five).
d. If five or fewer total exist in the population, select the whole population.

Also provide supporting evidence of the sampling process used including: (1) full population, (2) samples selected, and (3) output from the statistical function used to perform the sampling (e.g. RAT-STATS output).

File(s) Contents	*File Name / Page(s)*
Full Population	
Samples Selected	
Statistical Function Output	
Comments	

9. Per Requirement R1.2, for each item selected in the sample from step 8 above, provide any existing documented analysis as to why the asset was categorized as a "Medium Impact Cyber System." Please also ensure that you include which criteria were met within Attachment 1.

Medium Impact Cyber System Analysis	
Filename	
Comments	

Was each sample identified as a Medium Impact BES Cyber System according to Attachment 1, Section 2?

☐ Yes.
☐ No, respond "Not Compliant" for R1 to the Self-Certification in webCDMS.

10. Per Requirement R1.3, provide a list of BES Assets that contain Low Impact BES Cyber System(s).

BES Assets containing Low Impact BES Cyber System(s)	
Filename	
Comments	

11. For any BES Assets that meet the Attachment 1 High or Medium Impact Criteria, but do not contain High or Medium Impact BES Cyber Systems, list them below and provide a brief narrative describing why (add additional rows if necessary):

BES Asset	Narrative

380 St. Peter Street, Suite 800, Saint Paul, MN 55102 MidwestReliability.org P. 651.855.1760 F. 651.855.1712

Document Submittals

MRO requires copies of the following be submitted with the Part 1 self-certification response:

a) BES Cyber System Categorization Count Documentation

MRO requires copies of the following be submitted with the Part 2 self-certification response:

b) BES Cyber System Categorization Process Document
c) Updated Facility Verification Form
d) List of your High Impact BES Cyber Systems
e) Samples selected of your High Impact BES Cyber Systems
f) Output from the statistical function used to perform the sampling of your High Impact BES Cyber Systems (e.g. RAT-STATS output).
g) For each sampled High Impact BES Cyber System, existing documented analysis as to why the asset was categorized as a "High Impact Cyber System"
h) List of your Medium Impact BES Cyber Systems
i) Samples selected of your Medium Impact BES Cyber Systems
j) Output from the statistical function used to perform the sampling of your Medium Impact BES Cyber Systems (e.g. RAT-STATS output).
k) For each sampled Medium Impact BES Cyber System, existing documented analysis as to why the asset was categorized as a "Medium Impact Cyber System"
l) BES Assets containing Low Impact BES Cyber System(s)

Please make sure to use unique file names for each evidence file submitted, and identify within your responses to the steps above which specific evidence files support each conclusion made. These references and the use of unique file names helps Facilitate and expedite MRO's review of the Self-Certification work that has been performed.

All other data related to the registered entity's analysis and self-certification response are to be retained for at least 180 days after the submission date. MRO staff may request submission of additional information at a later date, on a random basis, to verify accuracy of self-certification submittals.