NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

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

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

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).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

Registered Entity Response (Required):

Question 1: Do you share compliance responsibility for this Requirement with another entity? ☐ Yes ☐ No

For example, is any BES Cyber System located at a shared facility?

If "Yes," list the following for each asset for which compliance responsibility is shared:

- Asset name or designation
- Joint Registration Organization (JRO), Coordinated Functional Registration (CFR), or other document describing the shared compliance responsibility, if any
- Other information regarding the shared compliance responsibility which may be useful to the audit team in determining the appropriate audit scope and approach for the asset

Note: A separate spreadsheet or other document may be used to provide all or part of this information. If so, provide the document reference below.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Initial Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
The process implemented per R1 that considers each of the asset types listed in R1 i through vi to identify and

assigns an impact rating to BES Cyber Systems.

Evidence Set 1:

1. A list of all assets for which you are responsible for compliance for this Requirement, per CIP-002-5.1 Section 4, Applicability. Include in this list the following:
    a. Identification (name, number, etc.) of the asset.
    b. The type of asset (generation resource, substation, etc.).
        i. If compliance responsibility for BES Cyber Systems at this asset is shared, describe the circumstances of the shared responsibility.
    c. An indication if there is a high impact BES Cyber System at the asset.
    d. An indication if there is a medium impact BES Cyber System at the asset.
    e. An indication if there is a low impact BES Cyber System at the asset.
    f. If the asset was commissioned during the audit period, the date of commissioning.
    g. If the asset was de-commissioned during the audit period, the date of de-commissioning.
2. A list of all high impact BES Cyber Systems identified, and the asset(s) with which the BES Cyber System is associated.
3. A list of all medium impact BES Cyber Systems identified, and the asset(s) with which the BES Cyber System is associated.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of assets and BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of assets provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of assets which contain high or medium impact BES Cyber Systems. For this sample of assets, provide the following:
    a. A list of high impact BES Cyber Systems, for which this entity has full or partial compliance responsibility, used by and located at the asset
    b. A list of medium impact BES Cyber Systems associated with the asset for which this entity has full or partial compliance responsibility
    c. A list of all BES Cyber Assets associated with each high or medium impact BES Cyber System identified in a. or b. above.
    d. A list of all Cyber Assets (that are not BES Cyber Assets), if any, associated with each high or medium impact BES Cyber System identified in a. or b. above.
    e. Evidence that the process required by R1 was implemented to determine the list of high and medium impact BES Cyber Systems.
2. From the list of assets provided in response to Evidence Set 1, the Compliance Enforcement Authority will select a sample of assets which contain low impact BES Cyber Systems. For this sample of assets, provide the following:
    a. Evidence that the process required by R1 was implemented to determine the list of assets containing low impact BES Cyber Systems.
3. From the list of assets provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of assets which do not contain BES Cyber Systems. For this sample of assets, provide the following:
    a. Evidence that the process required by R1 was implemented and resulted in a determination of

no BES Cyber Systems.

4. From the list of high impact BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of high impact BES Cyber Systems. For this sample set, provide the following evidence:
   a. The rationale for the determination of the impact rating of the BES Cyber System.
5. From the list of medium impact BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of medium impact BES Cyber Systems. For this sample set, provide the following evidence:
   a. The rationale for the determination of the impact rating of the BES Cyber System.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-002-5.1, R1

This section to be completed by the Compliance Enforcement Authority

	Review the process implemented per R1 that considers each of the asset types listed in R1 i through vi to identify and assigns an impact rating to BES Cyber Systems. Perform the following: 1. Verify that the process considers each of the asset types listed in R1 i through vi. 2. Verify that the process contains provisions to ensure that all assets of each applicable type are considered. 3. Verify that the process can be reasonably expected to identify all high and medium impact BES Cyber Systems at each asset. 4. Verify that the process can be reasonably expected to assign the correct impact rating to each identified high and medium impact BES Cyber System at each asset. 5. Verify that the process can be reasonably expected to identify all assets which contain a low impact BES Cyber System.
	From Items 1, 2 and 3 provided in Evidence Set 1, select the following samples and submit these samples to the entity for creation of Evidence Set 2: 1. For Evidence Set 2 Item 1, a sample of assets which contain high and/or medium impact BES Cyber

	Systems. 2. For Evidence Set 2 Item 2, a sample of assets which contain low impact BES Cyber Systems. 3. For Evidence Set 2 Item 3, a sample of assets which do not contain BES Cyber Systems. 4. For Evidence Set 2 Item 4, a sample of high impact BES Cyber Systems. 5. For Evidence Set 2 Item 5, a sample of medium impact BES Cyber Systems.
	From the evidence provided in response to Evidence Set 2 Item 1, for each asset in the sample: 1. Verify that the high and medium impact BES Cyber Assets associated with the sampled asset have been correctly identified. 2. Verify that the impact rating of each identified BES Cyber System is correct.
	From the evidence provided in response to Evidence Set 2 Item 2, for each asset in the sample: 1. Verify that the asset has been correctly identified as containing a low impact BES Cyber System.
	From the evidence provided in response to Evidence Set 2 Item 3, for each asset in the sample: 1. Verify that the sampled asset does not contain a BES Cyber System.
	From the evidence provided in response to Evidence Set 2 Item 4, for each BES Cyber System in the sample: 1. Verify that the BES Cyber Assets (and Cyber Assets, if any) comprising the BES Cyber System are identified. 2. Verify that the correct impact rating has been assigned to the BES Cyber System.
	From the evidence provided in response to Evidence Set 2 Item 5, for each BES Cyber System in the sample: 1. Verify that the BES Cyber Assets (and Cyber Assets, if any) comprising the BES Cyber System are identified. 2. Verify that the correct impact rating has been assigned to the BES Cyber System.

Notes to Auditor:

1. Results-based Requirement: The auditor should note that this is a results-based Requirement. As such, the entity has great latitude in determining how the result is achieved. The auditor should focus on verifying that the result is complete and correct.
2. Effective Date: The effective date of this requirement is April 1, 2016. See the Implementation Plan and any in-force transition guidance for additional information.
3. Considerations for virtual systems: The auditor should note that the Glossary of Terms defines Cyber Assets as, "Programmable electronic devices, including the hardware, software, and data in those devices. [Emphasis added]" In reviewing the identification of BES Cyber Systems, verify that the entity has identified the component BES Cyber Assets at the device level, and has included the hardware, software, and data in those devices.
    a. If the device is a computer system which operates a virtual environment, then the auditor should verify that the hypervisor and all client operating systems, applications, and data are considered to be part of the associated BES Cyber System and are protected accordingly.
    b. If the device is a network component within an ESP which meets the qualifications of a BES Cyber Asset, all data networks connected to the device must be protected at the same level as the associated BES Cyber System.
    c. If the device is a data storage system (SAN, etc.), the device and all data stored on it must be protected at the same level as the associated BES Cyber System.

Auditor Notes:

R2 Supporting Evidence and Documentation

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.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

Registered Entity Response:

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Initial Evidence Requested:

Provide the following evidence, or other evidence to demonstrate compliance.
Evidence of each review of the identifications in Requirement R1 during the audit period.
Evidence of the approval by the CIP Senior Manager or delegate of the identifications in Requirement R1 during the audit period.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-002-5.1, R2

This section to be completed by the Compliance Enforcement Authority

	Verify the reviews of the identifications in Requirement R1 have occurred at least every 15 calendar months during the audit period.
	Verify the review of the identifications in Requirement R1 has occurred as required by "Implementation Plan for Version 5 CIP Cyber Security Standards."
	Verify the approvals by the CIP Senior Manager or delegate of the identifications in Requirement R1 have occurred at least every 15 calendar months during the audit period.
	Verify the approval by the CIP Senior Manager or delegate of the identifications in Requirement R1 has occurred as required by "Implementation Plan for Version 5 CIP Cyber Security Standards."

Notes to Auditor:

1. Effective Date: The effective date of this requirement is April 1, 2016. See the Implementation Plan and any in-force transition guidance for additional information.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-002-5.1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order No. 706
FERC Order No. 791

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Term	Acronym	Definition
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.
BES Cyber Asset		A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.

		Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.
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.
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.
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, CIP-002 through CIP-011.
Control Center		One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in realtime 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.
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.
Cyber Assets		Programmable electronic devices, including the hardware, software, and data in those devices.
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.
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.)
Interconnection Reliability Operating Limit		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.
Intermediate System		A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.
Nuclear Plant Licensing Requirements	NPLRs	Requirements included in the design basis of the nuclear plant and statutorily mandated for the operation of the plant, including nuclear power plant licensing requirements for:

		1. Off-site power supply to enable safe shutdown of the plant during an electric system or plant event; and 2. Avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.
Nuclear Plant Interface Requirements	NPIRs	The requirements based on NPLRs and Bulk Electric System requirements that have been mutually agreed to by the Nuclear Plant Generator Operator and the applicable Transmission Entities.
Protection System		Protection System – • Protective relays which respond to electrical quantities, • Communications systems necessary for correct operation of protective functions • Voltage and current sensing devices providing inputs to protective relays, • Station dc supply associated with protective functions (including batteries, battery chargers, and non-battery-based dc supply), and • Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.
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).
Real Power		The portion of electricity that supplies energy to the load.
Special Protection System (Remedial Action Scheme)	SPS	An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme.
System		A combination of generation, transmission, and distribution components.
Transient Cyber Asset		A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Cyber Asset within an ESP. Examples include, but are not limited to,

		Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Transmission		An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1v0	06/17/2014	Posted for Industry Comment	New Document

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.