NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers~~Control Center Communication Networks~~

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	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		
R2	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 RSAW may provide 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 reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which 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)

Registered Entity Response (Required):

Question 1[A1][A2]**:** Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the entity does not own or operate a Control Center.
   - ~~Evidence that the Registered Entity's asset list does not contain a Control Center.~~
2. The remainder of this RSAW may be left blank.

~~If yes, continue with Question 2.~~

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

~~**Question 2:** Is data used for Operational Planning Analysis, Real-time Assessments, or Real-time monitoring and control transmitted between Control Centers at any time by any Control Center owned or operated by the Registered Entity? ☐ Yes ☐ No~~

~~If no:~~

1. ~~Provide evidence in the space below supporting this assertion. This evidence may include, but is not limited to:~~
   - ~~Evidence demonstrating data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring and control is not transmitted between Control Centers at any time by any Control Center owned or operated by the Registered Entity.~~
2. ~~The remainder of this RSAW may be left blank.~~

~~If yes, continue with the remainder of this RSAW.~~

~~[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]~~

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

1.2 Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3 Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

~~The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**1.1** Risk mitigation shall be accomplished by one or more of the following actions:~~

- ~~Physically protecting the communication links transmitting the data;~~
- ~~Logically protecting the data during transmission; or~~
- ~~Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.~~

~~Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.~~

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

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.

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-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to ~~either~~ Question 1 ~~or Question 2~~, verify~~:~~ ~~The~~the Registered Entity does not own or operate a Control Center. Note: If the Registered Entity does not own or operate a Control Center, the remainder of this RSAW is not applicable.~~; or~~ ~~The Registered Entity does not transmit data used for Operational Planning Analysis, Real-time Assessments, or Real-time monitoring and control at any time between Control Centers.~~
	Verify the entity has developed one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers.~~; and~~
	~~If the Registered Entity has answered "Yes" to Question 2, verify:~~ ~~The entity has developed one or more documented plans to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring and control data while being transmitted between Control Centers; and~~ ~~The documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers; and~~ ~~The documented plans collectively include identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and~~ Verify the ~~The~~ documented plans collectively include identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities. ~~The documented plan(s) collectively address all data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring transmitted between Control Centers; and~~ ~~The documented plan(s) collectively accomplish risk mitigation by one or more of the following actions:~~ ~~Physically protecting the communication links transmitting the data;~~ ~~Logically protecting the data during transmission; or~~ ~~Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.~~
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
Note to Auditor: 1. Oral communications are not in scope for CIP-012-1.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation to demonstrate implementation of methods to mitigate the risk of the unauthorized disclosure or modification of data in Requirement R1.

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.

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-012-1, R2

This section to be completed by the Compliance Enforcement Authority

	~~If the Registered Entity has answered "Yes" to Question 2, verify with system-generated evidence (where available) that the Registered Entity has implemented the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.~~
	Verify the entity has implemented one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has identified security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has identified demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers;

	and
	Verify the entity has identified roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "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 822 P53-56, 58, and 62

Selected Glossary Terms

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

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

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.

~~Operational Planning Analysis~~

~~An evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation shall reflect applicable inputs including, but~~

~~not limited to, load forecasts; generation output levels; Interchange; known Protection System and Special Protection System status or degradation; Transmission outages; generator outages; Facility Ratings; and identified phase angle and equipment limitations. (Operational Planning Analysis may be provided through internal systems or through third-party services.)~~

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time

Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Tas~~f~~k Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force	Response to comments: • RF: Footnote 1 page 1 added space after "references." • RF: Changed "Tasf" to "Task" in Revision History • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.