NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-008-5 – Cyber Security — Incident Reporting and Response Planning

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		
R3	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			
P1.1			
P1.2			
P1.3			
P1.4			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			
P3.2			

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 document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

R1 Part 1.1

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

Registered Entity Response (Required):

Question: Is Part 1.1 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any high impact or medium impact BES Cyber Systems.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for compliance with this Part. The processes should collectively cover the identification, classification, and response to a Cyber Security Incident.
List of all BES Cyber Systems identified as an Applicable System.

List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
List of all EACMS, PACS, and PCA associated with each BES Cyber System identified as an Applicable 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-008-5, R1, Part 1.1
This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Requirement to this entity. If the Requirement is not applicable, skip the remaining items in this list.
	Verify the process or processes provided have specific criteria to identify Cyber Security Incidents.
	Verify the process or processes provided have specific criteria to classify Cyber Security Incidents.
	Verify the process or processes provided have specific actions to respond to a Cyber Security Incident.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R1 Part 1.2

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

Registered Entity Response (Required):

Question: Is Part 1.2 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any high impact or medium impact BES Cyber Systems.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for compliance with this Part. The processes should collectively cover: 1. The means of determining Reportable Cyber Security Incidents. 2. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. If notification to the ES-ISAC is prohibited by law, provide the specific law and its applicability to the Responsible Entity.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
List of all identified Cyber Security Incidents including the identification date and time. If there were no

identified Cyber Security Incidents during the audit period, provide attestation to that effect.
List of all Reportable Cyber Security Incidents including the identification date and time. If there were no identified Cyber Security Incidents during the audit period, provide attestation to that effect.
Provide documentation, that includes the date and time of report, of all Reportable Cyber Security Incidents.

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-008-5, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the process or processes provided have specific criteria to identify Reportable Cyber Security Incidents.
	Verify the process or processes provided have specific and accurate information and instructions for contacting the ES-ISAC.
	Verify that all Reportable Cyber Security Incidents were reported to the ES-ISAC within one hour of discovery.
	Verify that all identified Cyber Security Incidents which were not reported to the ES-ISAC did not meet the definition of a Reportable Cyber Security Incident. See Note 1.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. Refer to the NERC Glossary of Terms and other evidence such as outage reports to determine if a Cyber Security Incident meets the definition of a Reportable Cyber Security Incident.

Auditor Notes:

R1 Part 1.3

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

Registered Entity Response (Required):

Question: Is Part 1.3 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any high impact or medium impact BES Cyber Systems.

☐ Other: [Provide explanation below]

[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plans or processes for compliance with this Part. The plans or processes should collectively cover the identification of the roles and responsibilities of groups or individuals responsible for responding to a Cyber Security Incident.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable 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**	**Document**	**Relevant**	**Description of Applicability**

		or Version	Date	Page(s) or Section(s)	of Document

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

Compliance Assessment Approach Specific to CIP-008-5, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the plans or processes define different roles for Cyber Security Incident response, such as monitoring, reporting, and documenting.
	Verify the plans or processes specify who is responsible, either individually or by group, for each role defined. If responsibility has been specified by group, then verify that each member of the group has been assigned a role.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R1 Part 1.4

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

Registered Entity Response (Required):
Question: Is Part 1.4 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity does not have any high impact or medium impact BES Cyber Systems.
☐ Other: [Provide explanation below]
[Note: A separate spreadsheet or other document may be used. 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented procedures for compliance with this Part. The procedures should collectively cover specific tasks for handling Cyber Security Incidents.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable 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-008-5, R1, Part 1.4
This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the procedures provided have specific actions that are to be performed in the event of a Cyber Security Incident.
	Verify the procedures address: 1. Various types of threats such as malware, unauthorized access, and denial of service. 2. Incident handling procedures such as containment, eradication, and resolution.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

R2 Part 2.1

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

Registered Entity Response (Required):

Question: Is R2 Part 2.1 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any High Impact or Medium Impact BES Cyber Systems.

☐ Other: [Provide explanation 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.

All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
For plan(s) that have identified roles and responsibilities by groups, provide the individual members of each group.
Evidence the Cyber Security Incident response plan has been tested at least once every 15 calendar months covering the entire 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-008-5, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the Cyber Security Incident response plan has been tested at least once every 15 calendar months.
	Verify the testing method is one of the following: • A response to an actual Reportable Cyber Security Incident. o Verify there is documentation of the incident report. o Verify the Cyber Security Incident response followed the Reportable Cyber Security Incident response plan(s). • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident. o Verify the drill or exercise included all individuals listed as having roles to respond to Cyber Security Incidents. o Verify there is documentation demonstrating that the plan(s) was exercised. • With an operational exercise of a Reportable Cyber Security Incident. o Verify the drill or exercise included all groups (and each member of the group) and all individuals listed as having roles to respond to Cyber Security Incidents. o Verify there is documentation demonstrating that the plan(s) was exercised.
	If any of the “verify” steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

Auditor Notes:

R2 Part 2.2

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.

Registered Entity Response (Required):

Question: Is R2 Part 2.2 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any High Impact or Medium Impact BES Cyber Systems.

☐ Other: [Provide explanation 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
Evidence the Cyber Security Incident response plan was used to respond to a Reportable Cyber Security Incident and/or the plan was used during an exercise of a Reportable Cyber Security Incident.
Evidence of any deviation from the Cyber Security Incident response plan during response to a Reportable Cyber Security Incident and/or during an exercise of a Reportable Cyber Security Incident.

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**	**Document Date**	**Relevant Page(s)**	**Description of Applicability of Document**

		Version		or Section(s)	

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

Compliance Assessment Approach Specific to CIP-008-5 R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the Cyber Security Incident response plan was used at least once every 15 calendar months for either an exercise of or in response to a Reportable Cyber Security Incident.
	Verify that, during the use of the Cyber Security Incident response plan, all deviations from the plan were documented.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Note to Auditor:

1. An attestation that no deviations occurred is unnecessary, since every task in the procedure should be verified as having been completed. If every task in the procedure was not completed, or some other action was performed, it should be documented.

Auditor Notes:

R2 Part 2.3

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.).	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

Registered Entity Response (Required):

Question: Is R2 Part 2.3 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any High Impact or Medium Impact BES Cyber Systems.

☐ Other: [Provide explanation 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
Evidence of all records related to Reportable Cyber Security Incidents.

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-008-5, R2, Part 2.3
This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify records related to Reportable Cyber Security Incidents are being retained. Types of records to verify: • Discovery method • Logs • Notes • Voice recordings • Police reports • Emails • Restoration records • Cyber Security Incident response plan usage checklists • Post-incident review notes
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

R3 Part 3.1

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.2.1. Document any lessons learned or document the absence of any lessons learned; 3.2.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.2.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Question: Is R3 Part 3.1 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any High Impact or Medium Impact BES Cyber Systems.

☐ Other: [Provide explanation 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
All versions of the Cyber Security Incident response plan(s) covering the audit period.
For plan(s) that have identified roles and responsibilities by groups, provide the individual members of each group.
Evidence, for tests of the Cyber Security Incident response plan(s), lessons learned were documented or the lack of any lessons learned was documented.
Evidence, for responding to a Reportable Cyber Security Incident, lessons learned were documented or the lack of any lessons learned was documented.
Evidence, for tests of the Cyber Security Incident response plan(s), the Cyber Security Incident response plan(s) were updated based on documented lessons learned associated with the plan.
Evidence, for a Reportable Cyber Security Incident, the Cyber Security Incident response plan(s) were updated based on documented lessons learned associated with the plan(s).
Evidence, for tests of the Cyber Security Incident response plan(s), any updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).
Evidence, for a Reportable Cyber Security Incident, any updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).

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-008-5, R3, Part 3.1
This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that within 90 calendar days of completing a test of the Cyber Security Incident response plan(s), lessons learned were documented or the lack of any lessons learned was documented.
	Verify that within 90 calendar days of responding to a Reportable Cyber Security Incident, lessons learned were documented or the lack of any lessons learned was documented.
	Verify that within 90 calendar days of completing a test of the Cyber Security Incident response plan(s), the Cyber Security Incident response plan(s) were updated based on documented lessons learned associated with the plan(s). See Note 1.
	Verify that within 90 calendar days of responding to a Reportable Cyber Security Incident, the Cyber Security Incident response plan(s) were updated based on documented lessons learned associated with the plan(s). See Note 1.
	Verify that within 90 calendar days of completing a test of the Cyber Security Incident response plan(s), any updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).
	Verify that within 90 calendar days of responding to a Reportable Cyber Security Incident, any updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor: 1. Corroborate evidence provided with versions of the plan and the documented lessons learned, if any.	

Auditor Notes:

R3 Part 3.2

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Question: Is R3 Part 3.2 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any High Impact or Medium Impact BES Cyber Systems.

☐ Other: [Provide explanation 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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for compliance with this Part.
List of all BES Cyber Systems identified as an Applicable System.
List of all BES Cyber Assets associated with each BES Cyber System identified as an Applicable System.
All versions of the Cyber Security Incident response plan(s) covering the audit period.
For plan(s) that have identified roles and responsibilities by groups, provide the individual members of each group.

Evidence, for a change to the roles or responsibilites, the Cyber Security Incident response plan(s) were updated.
Evidence, for a change to the Cyber Security Incident response groups or individuals, the Cyber Security Incident response plan(s) were updated.
Evidence, for a change to technology that the Responsible Entity determines would impact the ability to execute the plan(s), the Cyber Security Incident response plan(s) were updated.
Evidence, for a change to the roles or responsibilities, updates to the plan(s) were communicated to all groups or individuals with a defined role in the Cyber Security Incident response plan(s).
Evidence, for a change to the Cyber Security Incident response groups (and each member of the groups) or individuals, updates to the plan(s) were communicated to all groups or individuals with a defined role in the Cyber Security Incident response plan(s).
Evidence, for a change to technology that the Responsible Entity determines would impact the ability to execute the plan(s), updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).

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-008-5, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify that within 60 calendar days of a change to the roles or responsibilities, the Cyber Security Incident response plan(s) was updated.
	Verify that within 60 calendar days of a change to the Cyber Security Incident response groups or individuals, the Cyber Security Incident response plan(s) was updated.
	Verify that within 60 calendar days of a change to technology that the Responsible Entity determines would impact the ability to execute the plan(s), the Cyber Security Incident response plan(s) was updated.

	Verify that within 60 calendar days of a change to the roles or responsibilities, updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).
	Verify that within 60 calendar days of a change to the Cyber Security Incident response groups or individuals, updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).
	Verify that within 60 calendar days of a change to technology that the Responsible Entity determines would impact the ability to execute the plan(s), updates to the plan(s) were communicated to all groups (and each member of the groups) or individuals with a defined role in the Cyber Security Incident response plan(s).
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-008-5 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

See FERC Order 706
See FERC Order 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.

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.