NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-011-2 – Cyber Security – Information Protection

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			
P1.1			
P1.2			
R2			
P2.1			
P2.2			

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 implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

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 of the Applicable 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 information protection program(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.
List of all EACMS and PACS associated with each BES Cyber System identified as an Applicable System.
Evidence of implementation of each protection program that is used to meet this Part.

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-011-2, R1.1

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 information protection program(s) include method(s) to identify BES Cyber System Information.
	Verify each program has been implemented.

	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Notes to Auditor:

1. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.
2. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
3. Identification methodology should be capable of identifying information such as ESP drawings, lists of BES Cyber Assets and their IP addresses, configuration settings for firewalls and routers, physical security plans, etc.
4. Corroborate the implementation of the information protection program(s)'s identification method(s) with the training that is required by CIP-004-6, Requirement 2, Part 2.1.5.

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 and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Registered Entity Response (Required):
Question: Is R1.2 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity does not have any of the Applicable 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.
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 and PACS associated with each BES Cyber System identified as an Applicable System.
All applicable documented information protection program(s) for compliance with this Part.
Evidence of implementation of each protection program that is used to meet this Part.

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-011-2, R1.2

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 information protection program(s) include procedure(s) to protect and secure BES Cyber System Information, including storage, transit, and use.
	Verify each program has been implemented.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Notes to Auditor:

1. This requirement requires procedure(s) for the protection and secure handling of BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.
2. The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented.
3. The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information.
4. A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties.
5. Corroborate the implementation of the information protection program(s)'s protection and secure handling procedure(s) with the training that is required by CIP-004-6, Requirement 2, Part 2.1.5.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

Registered Entity Response (Required):
Question: Is Part 2.1 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity does not have any of the Applicable 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.

Initial Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented process(es) 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.
List of all EACMS, PACS, and PCA associated with each BES Cyber System identified as an Applicable System.
Evidence of implementation of each process.
Evidence Set 1: 1. List of Cyber Assets that have been reused with the exception of Cyber Assets that have been redeployed to systems in the Applicable Systems column. 2. List of Cyber Assets that have been returned to the manufacturer or a third-party, prior to reuse.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems, EACMS, and PACS to be used for the evidence requested below:
Evidence Set 2: 1. Evidence that each reused sampled BES Cyber System, EACMS, and PACS has been reused in accordance with this Part, including: a. the date the system or component of the system was removed from service. b. the individual who removed the system or component. c. the date the system or component of the system was purged or retained the system prior to reuse. d. the individual who purged or retained the system or component of the system prior to reuse. e. the method of purging or retaining.

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-011-2, R2.1

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 documented process(es) define the methods and specific processes used to preserve BES Cyber System Information confidentiality.
	Verify each documented process has been implemented.
	Verify each system or component of a system has been purged or retained.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Notes to Auditor:

1. For the sampling of Evidence Set 1 to derive the list of systems which are the subject of Evidence Set 2, a judgmental sample is strongly recommended. The audit team should focus on higher risk systems, but not exclude all lower risk systems.
2. If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.
3. Corroborate the implementation of the process(es) used to preserve the confidentiality of BES Cyber System Information with the training that is required by CIP-004-6, Requirement 2, Part 2.1.5.
4. Reconcile systems listed as applicable to this Part with previous lists of systems and the lists of disposed and reused systems.

Auditor Notes:

R2 Part 2.2

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

Registered Entity Response (Required):

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

If "No," why not?

☐ This entity does not have any of the Applicable 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 process(es) 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.
List of all EACMS, PACS, and PCA associated with each BES Cyber System identified as an Applicable System.
Evidence of implementation of each process.
Evidence Set 1: 1. List of Cyber Assets that have been disposed. 2. List of Cyber Assets that have been returned to the manufacturer or a third-party.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems, EACMS, and PACS to be used for the evidence requested below:
Evidence Set 2: 1. Evidence that each disposed sampled BES Cyber System, EACMS, and PACS has been disposed in accordance with this Part, including: a. the date the system or component of the system was removed from service. b. the individual who removed the system or component. c. the date the system or component of the system was purged, destroyed, or retained. d. the individual who purged, destroyed, or retained the system or component of the system. e. the method of purging, destroying, or retaining.

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-011-2, R2.2

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 documented process(es) define the methods and specific processes used to preserve BES Cyber System Information confidentiality.
	Verify each documented process has been implemented.
	Verify each system or component of a system has been purged, destroyed, or retained.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

Notes to Auditor:

1. For the sampling of Evidence Set 1 to derive the list of systems which are the subject of Evidence Set 2, a judgmental sample is strongly recommended. The audit team should focus on higher risk systems, but not exclude all lower risk systems.
2. If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain

documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

3. Corroborate the implementation of the process(es) used to preserve the confidentiality of BES Cyber System Information with the training that is required by CIP-004-6, Requirement 2, Part 2.1.5.
4. Reconcile systems listed as applicable to this Part with previous lists of systems and the lists of disposed and reused systems.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-004-6 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.