

**Reliability Standard Audit Worksheet[[1]](#footnote-1)**

# CIP-011-3 – 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]](#footnote-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 |  |  |

**\*** CIP-011-3 is only applicable to DPs that own certain UFLS, UVLS, RAS, Protection Systems, or Cranking Paths. See CIP-011-3 Section 4, Applicability, for details.

**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 |

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)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Note on Early Implementation**

In the December 7, 2021, Letter Order in Docket No. RM21-6-000, FERC approved CIP-004-7, CIP-011-3, and the associated Implementation Plan.

The Implementation Plan provides for early adoption of CIP-004-7 and CIP-011-3 as follows:

**Implementation Plan**

**Project 2019-02 BES Cyber System Information Access Management**

**Reliability Standard CIP-004 and CIP-011**

Compliance Dates for Early Adoption of Revised CIP Standards

A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.

If a Responsible Entity elects to comply with CIP-004-7 and CIP-011-3 before the Effective Date of January 1, 2024, the Responsible Entity must notify all applicable Regional Entities prior to that date. Such notification must be in writing and must include the date that the Responsible Entity will begin compliance with CIP-004-7 and CIP-011-3. It is recommended, but not required, that the notification to the Regional Entities occur at least 90 days prior to the date compliance with CIP-004-7 and CIP-011-3 will begin. It is recommended, but not required, that this compliance date be the start of a calendar quarter.

For a Responsible Entity that has notified the applicable Regional Entities that it is complying early with the new requirements, the applicable Regional Entities will monitor according to the new requirements beginning on the date elected by the Responsible Entity. If the applicable Regional Entities identify a noncompliance with the new requirements, they will stop monitoring once they have a sufficient understanding of the Responsible Entity’s failure to comply with the new requirements. The applicable Regional Entities will not monitor the Responsible Entity according to the requirements of CIP-004-6 or CIP-011-2 after the Responsible Entity’s elected effective date of CIP-004-7 and CIP-011-3.

Until the FERC-approved Effective Date of the new requirements, January 1, 2024, the applicable Regional Entities will record the noncompliance under the previous versions of the Reliability Standards. For the new CIP-004 requirement, CIP-004-7 R6, the noncompliance will be recorded under CIP-004-6 Requirement R4. The CIP-011-3 requirements tie back to the CIP-011-2 requirements, so the noncompliance will be recorded under the corresponding CIP-011-2 requirement.

Mitigation for noncompliance with the new requirements must remediate the noncompliance according to the specifications in the new requirements.

**R1 Supporting Evidence and Documentation**

**R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified *in CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

**M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

**R1 Part 1.1**

| **CIP-011-3 Table R1 – Information Protection Program** | | | |
| --- | --- | --- | --- |
| **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 BCSI. | Examples of acceptable evidence may include, but are not limited to, the following:   * Documented method to identify BCSI from entity’s information protection program; or * Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity’s information protection program; or * Training materials that provide personnel with sufficient knowledge to recognize BCSI; or * Storage locations identified for housing BCSI in the entity’s information protection program. |

**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-011-3 R1, Part 1.1

***This section to be completed by the Compliance Enforcement Authority***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more information protection programs that have method(s) to identify BCSI. |
|  | Verify the Responsible Entity has implemented the method(s) to identify BCSI. |

Auditor Notes:

**R1 Part 1.2**

| **CIP-011-3 Table R1 – Information Protection Program** | | | |
| --- | --- | --- | --- |
| **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 | Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | Examples of acceptable evidence for on-premise BCSI include, but are not limited to, the following:   * Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use; or * Records indicating that BCSI is handled in a manner consistent with the entity’s documented procedure(s).   Examples of evidence for off-premise BCSI may include, but are not limited to, the following:   * Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or * Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or * Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements). |

**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-011-3 R1, Part 1.2

***This section to be completed by the Compliance Enforcement Authority***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more information protection programs that include method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. |
|  | Verify the Responsible Entity has implemented the method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. |
| **Notes to Auditor:**  Authorization of access to BCSI that pertains to BCS, EACMS, and PACS at the medium-without-ERC impact rating should be addressed in the information protection program.  CIP-004-7 R6 applies to provisioned access to BCSI. Other forms of access, if any, should be addressed by the information protection program. | |

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-011-3 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-011-3 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-011-3 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 BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media. | Examples of acceptable evidence may include, but are not limited to, the following:   * Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI 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 BCSI. |

**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-011-3 R2, Part 2.1

***This section to be completed by the Compliance Enforcement Authority***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media, prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column). |
|  | Verify that prior to the release for reuse of Cyber Assets of Applicable Systems that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity has taken action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media. |

Auditor Notes:

**R2 Part 2.2**

| **CIP-011-3 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 BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media. | Examples of acceptable evidence may include, but are not limited to, the following:   * 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 BCSI prior to the disposal of an applicable Cyber Asset. |

**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-011-3 R2, Part 2.2

***This section to be completed by the Compliance Enforcement Authority***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media, prior to the disposal of applicable Cyber Assets that contain BCSI. |
|  | Verify that, prior to the disposal of Cyber Assets of Applicable Systems that contain BCSI, the Responsible Entity has taken action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroyed the data storage media. |

Auditor Notes:

**Additional Information:**

Reliability Standard

The full text of CIP-011-3 may be found on the NERC website (www.nerc.com) under “Program Areas & Departments,” “Standards,” “One-Stop-Shop.”

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

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

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

**Sampling Methodology**

Sampling is essential for auditing compliance with NERC Reliability Standards because 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 “Note on Early Implementation,” above, regarding FERC approval of the Reliability Standard and its associated Implementation Plan.

Revision History for RSAW

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Reviewers** | **Revision Description** |
| v1 | 11/10/2022 |  | New RSAW |

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 version of the Reliability Standards, approved 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. 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. [↑](#footnote-ref-1)
2. Compliance Assessment Date(s): The date(s) the compliance assessment (on-site audit, off-site spot check, etc.) occurs. [↑](#footnote-ref-2)