NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Reliability Standard Audit Worksheet[1]

## CIP-013-1 – Cyber Security - Supply Chain Risk Management

***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 | X | | |
| **R2** | X | X | X | X | | X | | | X | X | | |
| **R3** | X | X | X | X | | X | | | X | X | | |
| **R4** | X | X | X | X | | X | | | X | X | | |
| **R5** | X | X | X | X | | X | | | X | X | | |

**Legend:**

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

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

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

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

## Findings

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

| Req. | Finding | Summary and Documentation | Functions Monitored |
|---|---|---|---|
| R1 | | | |
| R2 | | | |
| R3 | | | |
| R4 | | | |
| R5 | | | |

| 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 supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

**1.1.** The use of controls in BES Cyber System planning and development to:

**1.1.1.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and

**1.1.2.** Evaluate methods to address identified risk(s).

**1.2.** The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:

**1.2.1.** Process(es) for notification of vendor security events;

**1.2.2.** Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

**1.2.3.** Process(es) for disclosure of known vulnerabilities;

**1.2.4.** Coordination of response to vendor-related cyber security incidents;

**1.2.5.** Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

**1.2.6.** Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

**1.2.7.** Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

**M1.** Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for mitigating cyber security risks as specified in the Requirement; and (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management plan(s).

**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-013-1, R1**

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

| | |
|---|---|
| | Verify the Responsible Entity has documented one or more supply chain risk management plans that collectively address the controls specified in Part 1.1 and Part 1.2, for each applicable type of Cyber Asset. |
| | For each documented supply chain risk management plan, verify the Responsible Entity has implemented the plan as applicable. |
| **Note to Auditor:** | |

**Auditor Notes:**

## R2 Supporting Evidence and Documentation

**R2.** Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

**2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and

**2.2.** Obtaining CIP Senior Manager or delegate approval.

**M2.** Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s) and evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures as specified in the Requirement. Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

**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-013-1, R2**

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

| | |
|---|---|
| | Verify that the Responsible Entity performed a review of each of its supply chain security risk management plans. |

| | |
|---|---|
| | Verify that the Responsible Entity evaluated revisions to each plan to address any applicable new supply chain security risks and mitigation measures. |
| | Verify that the Responsible Entity updated, as necessary, each of its cyber security risk management plans to address applicable new supply chain security risks and mitigation measures. |
| | Verify that the CIP Senior Manager, or delegate, approved each of the cyber security risk management plans. |
| | Verify that the review and update of each of the supply chain security risk management plans occurred at least once every 15 calendar months. |
| **Note to Auditor:** | |

**Auditor Notes:**

## R3 Supporting Evidence and Documentation

**R3.** Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

- **3.1.** Operating System(s);
- **3.2.** Firmware;
- **3.3.** Commercially available or open-source application software; and
- **3.4.** Patches, updates, and upgrades to 3.1 through 3.3.

**M3.** Evidence shall include (i) a documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation that the entity performed the actions contained in the process to verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to installation on high and medium impact BES Cyber Systems.

**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-013-1, R3**

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

| | |
|---|---|
| | Verify the Responsible Entity has documented one or more process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and |

| | |
|---|---|
| | medium impact BES Cyber Systems:<br>1. Operating system(s);<br>2. Firmware;<br>3. Commercially available or open-source application software; and<br>4. Patches, updates, and upgrades to operating systems, firmware, commercially available application software, and open-source application software. |
| | For each documented process for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems, verify the Responsible Entity has implemented the process for the applicable BES Cyber Systems. |
| **Note to Auditor:** | |

**Auditor Notes:**

## R4 Supporting Evidence and Documentation

**R4.** Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

- **4.1.** Authorization of remote access by the Responsible Entity;
- **4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and
- **4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions.

**M4.** Evidence shall include (i) a documented process(es) for controlling vendor remote access as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation of authorization of vendor remote access; hard copy or electronic logs of vendor-initiated Interactive Remote Access and system-to-system remote access sessions; hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.

**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-013-1, R4**

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

| | |
|---|---|
| | Verify the Responsible Entity has documented one or more processes for controlling vendor remote access to high and medium impact BES Cyber Systems. Verify the processes collectively address, for |

| | |
|---|---|
| | both vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor, the following items:<br>1. Authorization of remote access by the Responsible Entity;<br>2. Logging and monitoring of remote access sessions to detect unauthorized activity; and<br>3. Disabling or otherwise responding to unauthorized activity during remote access sessions. |
| | For both vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor, verify the Responsible Entity has implemented authorization of remote access. |
| | For both vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor, verify the Responsible Entity has implemented logging and monitoring of remote access sessions to detect unauthorized activity. |
| | For both vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor, verify the Responsible Entity disabled or otherwise responded to unauthorized activity during remote access sessions. |
| **Note to Auditor:** | |

**Auditor Notes:**

## R5 Supporting Evidence and Documentation

**R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).

**M5.** Evidence may include, but is not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate for each cyber security policy.

**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-013-1, R5**

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

| | |
|---|---|
| | For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics:<br>1. Integrity and authenticity of software and firmware and any patches, updates, and upgrades to |

| | |
|---|---|
| | software and firmware; and<br>2. Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s). |
| | Verify each policy used to meet this Requirement has been reviewed at least once every 15 calendar months. |
| | Verify the CIP Senior Manager or delegate has approved each policy used to meet this Requirement at least once every 15 calendar months. |
| **Note to Auditor:** | |

**Auditor Notes:**

## Additional Information:

### Reliability Standard

The full text of CIP-013-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

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

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

### Sampling Methodology

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

### Regulatory Language

FERC Order No. 829

## Revision History for RSAW

| Version | Date | Reviewers | Revision Description |
|---|---|---|---|
| 1 | 01/30/2017 | CIP RSAW Development Team | New Document |
| | | | |
| | | | |