**[Registered Entity Name]**

**NERC ID: [NCRXXXXX]**

**CIP-013-1 – Cyber Security – Supply Chain Risk Management, R1-R2**

**1st Quarter 2022 Self-Certification**

# Instructions

1. Populate the cover page by adding your entity’s name and NERC identification number.
2. Complete thetasks listed under **Assessment Guidance**.
3. Log into **Align** and complete your self-certification response.
4. Submit via the Secure Evidence Locker (SEL):
   1. This completed Worksheet; and
   2. Specific evidence requested within this document. Please make sure to use unique file names for each evidence file submitted, and identify within your narratives which specific evidence files support each conclusion made. These references and the use of unique file names helps facilitate and expedite MRO’s review of the Self-Certification work that has been performed.
   3. Any internal control information related to the Reliability Standard and Requirement in scope with supporting documentation of design and implementation of the internal control(s).

# Scope

**CIP-013-1 – Cyber Security – Supply Chain Risk Management, R1 – R2**

***R1.*** *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:*

* 1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*
  2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*
     1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*
     2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*
     3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*
     4. *Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;*
     5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*
     6. *Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)*

***M1.*** *Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.*

***R2.*** *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

*Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.*

***M2.*** *Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.*

# Purpose:

To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

# Applicability:

* + 1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

## Balancing Authority

* + - 1. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
         1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

* + - * 1. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        2. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

## Generator Operator

* + - 1. **Generator Owner**
      2. **Reliability Coordinator**
      3. **Transmission Operator**
      4. **Transmission Owner**

# Assessment Guidance

**Requirement 1**

1. Provide the documented supply chain cyber security risk management plan(s) for high and/or medium impact BES Cyber Systems.

|  |  |  |
| --- | --- | --- |
| **Evidence of Supply Chain Cyber Security Risk Management Plan(s)** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. Provide the process(es) used in planning for the procurement of BES Cyber Systems. Please identify where the processes collectively result in the identification and assessment of cyber security risks to the BES from vendor products and services resulting from:
2. Procuring and installing vendor equipment and software; and
3. Transitions from one vendor or set of vendors to another vendor or set of vendors.

|  |  |  |
| --- | --- | --- |
| **Evidence of Process(es) to Identify and Assess Cyber Security Risks** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. Provide the process(es) used in the procurement of BES Cyber Systems. Please identify where the processes address the sub requirements identified in Requirement R1, Part 1.2.1 through Part R1.2.6. If any of the sub requirements identified in Part 1.2.1 through Part 1.2.6 were not applicable, provide evidence of the reason(s) it is not applicable.

|  |  |  |
| --- | --- | --- |
| **Evidence of Process(es) Used in the Procurement to Address R1.2 Topics** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. Do the documented supply chain risk management plan(s) evaluate the following vendor types with the identification and assessment of cyber security risks?
   * value-added resellers
   * service providers
   * open-source software providers, and
   * original equipment manufacturers.

No (If “no” proceed to the next step)

Yes (If “yes”, please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3 and the vendor types evaluated per the plan(s), or provide a brief narrative response.)

|  |  |  |
| --- | --- | --- |
| **Evaluation of Various Supplier Types** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Entity Narrative** | | |
| Response: | | |

1. Do the documented supply chain risk management plan(s) address renewal agreements, extensions, and/or service subscriptions?

No (If “no” proceed to the next step)

Yes (If “yes”, please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3 and how renewal agreements, extensions, and/or service subscriptions are addressed per the plan(s), or provide a brief narrative response.)

|  |  |  |
| --- | --- | --- |
| **Renewal Agreements, Extensions, and/or Services Subscriptions** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Entity Narrative** | | |
| Response: | | |

1. Do you utilize a third-party service to identify and assess cyber security risks of vendors?

No (If “no” proceed to the next step)

Yes (If “yes”, please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3 that describes how you assess the performance of the third-party assessment and how the results of your assessment are utilized, or provide a brief narrative response and briefly describe how the service supports the documented processes.)

|  |  |  |
| --- | --- | --- |
| **Use of Third-Party Service for Assessment** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Entity Narrative** | | |
| Response: | | |

1. If a vendor chooses not to adhere to one or more sub-parts of Part 1.2, please cite the process, corresponding page(s) or section(s) detailing what would occur, or provide a separate narrative describing the process(es) that would be followed for the applicable sub-part(s). Such as, a process to ensure notification, coordination, disclosure, etc. of vendor-identified incidents, vulnerabilities, terminated access, etc.

|  |  |  |
| --- | --- | --- |
| **Vendor Non-Adherence** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Entity Narrative** | | |
| Response: | | |

1. Do the documented supply chain risk management plan(s) address the implementation of emergency related procurements?

|  |  |  |
| --- | --- | --- |
| **Emergency Related Procurements** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Entity Narrative** | | |
| Response: | | |

**Requirement 2**

1. Provide a list of all individuals, companies, or external organizations the registered entity, or its affiliates, contract with to supply BES Cyber Systems and related services (*refer to the CIP Evidence Request Tool (version 5) – Request ID CIP-013-R2-L1-01*).

|  |  |  |
| --- | --- | --- |
| **Listing of Persons, Companies, or Other Organizations** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. Provide a list of each procurement of vendor products or services resulting from:
2. Procuring and installing vendor equipment and software; and
3. Transitions from one vendor(s) to another vendor(s) during the audit period for high and/or medium impact BES Cyber Systems, if applicable.

The listing should include:

1. Unique ID;
2. Associated BES Cyber System Impact Level;
3. Description;
4. If the Procurement was for Vendor Products; Vendor Services; and/or Resulted in Vendor Transition;
5. Identification & Assessment Start Date;
6. Identification & Assessment End Date;
7. Procurement Start Date;
8. Procurement End Date.

*\*\*Note\*\* - The listing of procurements should include those completed and in progress. This is requesting information that would be submitted with the CIP Evidence Request Tool’s Procurement tab request for information (version 5.0).*

|  |  |  |
| --- | --- | --- |
| **Listing of Procurements** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. Select a random sample from your full population identified in step 2 above using the following sampling logic. (A random sample can be selected using statistical functions available in Microsoft Excel or through use of RAT-STATS, a free sampling tool available from the U.S. Department of Health & Human Services Office of Inspector General.)

From the population:

* + - 1. Select at least 10% of the population (maximum number sampled 10) making sure at least five are sampled (e.g. if fewer than 50 exist in your population, select at least five).
      2. If five or fewer total exist in the population, select the whole population.

Also provide supporting evidence of the sampling process used including: (1) full population, (2) samples selected, and (3) output from the statistical function used to perform the sampling (e.g. RAT-STATS output). Depending on the sampling method/software used, a screenshot or creation of a PDF to capture the sampling output may be required.

|  |  |
| --- | --- |
| ***File(s) Contents*** | ***File Name / Page(s)*** |
| **Full Population** |  |
| **Samples Selected** |  |
| **Statistical Function Output** |  |
| **Comments** |  |

1. For each procurement selected in the sample above from (R2) step 3,
   1. Provide the following attribute information:
      1. Associated BES Cyber System Impact Level;
      2. Description;
      3. If the Procurement was for Vendor Products; Vendor Services; and/or Resulted in Vendor Transition;
      4. Identification & Assessment Start Date;
      5. Identification & Assessment End Date;
      6. Procurement Start Date;
      7. Procurement End Date; and
   2. Provide evidence of the identification and assessment of cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from:
2. Procuring and installing vendor equipment and software; and
3. Transitions from one vendor(s) to another vendor(s), if applicable.

|  |  |  |
| --- | --- | --- |
| **Evidence of Identification and Assessment of Cyber Security Risks** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. For each procurement selected in the sample above from (R2) step 3, related to the products or services provided that pose cyber security risk, provide evidence of the implemented processes used in procuring for the areas identified in Requirement R1 Part 1.2.1 through 1.2.6. As applicable, please identify where the process(es) specifically address:
   1. Notification by the vendor of vendor-identified incidents;
   2. Coordination of responses to vendor-identified incidents;
   3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
   4. Disclosure by vendors of known vulnerabilities;
   5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and
   6. Coordination of controls for:
      1. Vendor-initiated Interactive Remote Access, and
      2. System-to-system remote access with a vendor(s).

*\*\*Note\*\* - If any of the areas are not applicable to the procurement, provide evidence to demonstrate the reason(s) it is not applicable.*

|  |  |  |
| --- | --- | --- |
| **Evidence of Addressing R1.2 Topics in Procurements** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. How are the procurements and applications of Requirement R1 supply chain risk management plan(s) documented and verified? Please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3, or provide a narrative describing how procurements and implementation of the plan(s) are documented for evidentiary purposes.

|  |  |  |
| --- | --- | --- |
| **How Plan Implementation and Procurements are Evidenced** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| **Entity Narrative** | | |
| Response: | | |

1. Are vendor risk assessments routinely monitored and updated, regardless of procurement activities?

No (If “no” proceed to the next step)

Yes (If “yes”, please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3, or provide a brief narrative response describing this process.) If “yes”, please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3 that describes how you routinely monitor and update vendor risk assessments, or provide a brief narrative response.)

|  |  |  |
| --- | --- | --- |
| **Vendor Risk Assessments** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. Since October 1, 2020, have there been any applicable transitions from one vendor(s) to another vendor(s)? If so, please briefly describe.

|  |
| --- |
| **Entity Narrative** |
| Response: |

1. How are vendor relationships; including updates and/or communications, documented? Please cite the process, corresponding page(s) or section(s) references to a file provided under Requirement 1 Step 1-3, or provide a narrative describing how vendor relationships; including updates and/or communications, documented.

|  |  |  |
| --- | --- | --- |
| **Vendor Documentation** | | |
| **Filename(s)** | **Document Title** | **Relevant Page(s) or Section(s)** |
|  |  |  |
|  |  |  |
|  |  |  |
| |  | | --- | | **Entity Narrative** | | Response: | | | |

1. For procurements that do not meet the applicability of CIP-013 Requirement 1, are any of the supply chain risk management plan(s) protections afforded? If so, please briefly describe. *Note: A response is not mandatory to this question.*

|  |
| --- |
| **Entity Narrative** |
| Response: |

# Compliance

Is there adequate documentation in place to support Requirement 1, steps 1-8 and Requirement 2, steps 1-10?

Yes, respond “Compliant” for R1 and R2 to the Self-Certification in Align. Include comments supporting the “Compliant” response. Upload supporting documentation to the SEL.

No, respond “Not Compliant” for R1 and R2 to the Self-Certification in Align. Include comments supporting the “Not Compliant” response. Upload supporting documentation to the SEL.

# Document Submittals

MRO requires copies of the following be submitted with the self-certification response:

1. This worksheet and
2. Supporting documentation referenced in the Assessment Guidance.
3. Additional internal control information including implementation evidence

Please make sure to use unique file names for each evidence file submitted, and identify within your responses to the steps above which specific evidence files support each conclusion made. These references and the use of unique file names helps facilitate and expedite MRO’s review of the Self-Certification work that has been performed.

All other data related to the registered entity’s analysis and self-certification response are to be retained for at least 180 days after the submission date. MRO staff may request submission of additional information at a later date to verify accuracy of self-certification submittals.