**[Registered Entity Name]**

**NERC ID: [NCRXXXXX]**

**CIP-009-6 - R1, R2**

**1st Quarter 2023 Self-Certification**

# Instructions

1. Populate the cover page by adding your entity’s name and NERC identification number.
2. Download CIP-009-6 from NERC’s website (optional for reference):

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-009-6.pdf>

1. Complete thetasks listed under **Assessment Guidance** in this document.
2. Log into **Align** and complete your self-certification response (see Section [9.0 Self-Certifications](https://training.nerc.net/Home/ViewApplicationVideos?system=Align&role=Registered%20Entities)).
3. Submit via the ERO Secure Evidence Locker (ERO SEL) Site:
   1. This completed Worksheet;
   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 response made. These references and the use of unique file names help facilitate and expedite MRO’s review of the Self-Certification work that has been performed; and
   3. Any internal control information related to the Reliability Standard and Requirement(s) in scope with supporting documentation of design and implementation of the internal control(s).

# Scope:

The scope for this Self-Certification is CIP-009-6 - R1 & R2. Each Responsible Entity shall include the data from the monitoring period between May 1, 2021 – September 30, 2022 as applicable for each step in the Assessment Guidance below.

# Assessment Guidance

**R1 Step #1 - Recovery Plan Specifications**

Per Requirement R1, provide recovery plan document(s) for High and Medium Impact BES Cyber Systems and associated EACMS and PACS. Ensure the documents address all sections of CIP-009-6 Table R1 – *Recovery Plan Specifications*

**CIP-009-6 R1 – Recovery Plan Specifications**

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **File Name** | **Location within document/Page number** | **Comments/Explanation** |
| **Part 1.1 -** Conditions for activation of the recovery plan(s). |  |  |  |
| **Part 1.2 -** Roles and responsibilities of responders. |  |  |  |
| **Part 1.3 -** One or more processes for the backup and storage of information required to recover BES Cyber System  functionality. |  |  |  |
| **Part 1.4 -** One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures. |  |  |  |
| **Part 1.5 -** One or more processes to preserve data, per Cyber Asset capability, for  determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery. |  |  |  |

1. **Recovery Plan Specification Internal Control(s)**

Required (Provide information for Option 1 or Option 2):

The internal controls options provided below are meant to allow registered entities to choose their best approach to provide their internal control information. **Option 1** is to allow registered entities to provide their information as they see applicable and in their format. **Option 2** is to assist registered entities with specific questions on how it is reaching reasonable assurance for compliance to CIP-009-6 - R1.

***Option 1:***

Provide information that shows:

1. Internal controls incorporation into global program for CIP-009-6 - R1
2. Internal controls design (process, procedures, etc. ...)
3. Internal controls implementation/operational evidence (control tests or evidence showing execution of the internal controls indicated)

Please indicate in this table:

|  |  |
| --- | --- |
| **All Internal Control(s) related to CIP-009-6 - R1** | |
| **Global Program Filename(s)** |  |
| **Comments** |  |
| **Internal Controls Design Filename(s)** |  |
| **Comments** |  |
| **Internal Controls Implementation and/or Operational Evidence Filename(s)** |  |
| **Comments** |  |

***Option 2:***

The following questions may be used as an approach to address internal controls for CIP-009-6 - R1.

*Note: These questions are similar to those used by MRO in audit engagements. If a process or the implementation is not documented, provide comments about internal control(s) and indicate “not applicable” in supporting evidence fields*.

1. Requirement 1.1

How do you help ensure that the documents are kept up to date?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. Requirement 1.2
   1. How often are the roles and responsibilities reviewed to ensure that they are adequately filled?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. Does your plan include alternates for each role and responsibility?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. Requirement 1.3

How do you ensure all methods of backup and storage are included in plans?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. Requirement 1.4
   1. How do you know whether backups are complete?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. When a backup fails, how do you inform stakeholders of failures?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. Requirement 1.5
   1. How do you document preservations?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. How are SMEs trained on methods to preserve data?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. If there are internal controls that are not addressed in the internal control questions above for CIP-009-6 - R1, please explain in detail and provide supporting evidence if available.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence of Process Filename(s)** |  |
| **Supporting Evidence of Implementation Filename(s)** |  |

Was each Part in **R1 Step 1** shown to follow the appropriate procedure/process in accordance with NERC Standard CIP-009-6 R1?

☐ Yes, respond “Compliant” for R1 to the Self-Certification in Align. Include a comment summary and upload supporting documentation to the ERO SEL.

☐ No, respond “Not Compliant” for R1 to the Self-Certification in Align. Include a comment summary based on potential issues and upload supporting documentation to the ERO SEL.

☐ Do not own, respond “Do Not Own” for R1 to the Self-Certification in Align. Include comments supporting the “Do Not Own” response and upload supporting documentation to the ERO SEL.

☐ Do not meet the applicability requirements of the full standard, respond “Not Applicable” for R1 to the Self-Certification in Align. Include comments supporting the “Not Applicable” response and upload supporting documentation to the ERO SEL. This response should not be used if the circumstance within the standard or requirement language did not happen. This response should only be used if the requirement or standard is not applicable at all to the entity (such as not registered for the function).

**R2 Step 1 - Recovery Plans Testing and Implementation**

Per Requirement R2 – Part 2.1, provide evidence of testing the recovery plans referenced in Requirement R1 at least every 15 calendar months:

* + By recovering from an actual incident;
  + With a paper drill or tabletop exercise; or
  + With an operational exercise

|  |  |
| --- | --- |
| **Recovery Plan Implementation and Testing** | |
| **Filename** |  |
| **Comments** |  |

**R2 Step 2 - Test a Representative Sample**

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3

Select a random sample from your population 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.

**Recovery Plan Implementation and Testing**

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

**R2 Step 3 - Test Recovery Plans**

Per Requirement R2 – Part 2.3, provide evidence of testing the recovery plans referenced in Requirement R1 at least every 36 calendar months:

* An actual recovery response may substitute for an operational exercise.

|  |  |
| --- | --- |
| **Recovery Plan Implementation and Testing** | |
| **Filename** |  |
| **Comments** |  |

1. **Recover Plan Implementaion and Testing Internal Control(s)**

Required (Provide information for Option 1 or Option 2):

The internal controls sections provided below are meant to allow entities to choose their best approach to provide their internal control information. Option 1 is to allow registered entities to provide their information as they see applicable and in their format. Option 2 is to assist registered entities with specific questions on how it is reaching reasonable assurance for compliance to CIP-009-6 - R2.

***Option 1:***

Provide information that shows:

1. Internal controls incorporation into global program for CIP-009-6 - R2
2. Internal controls design (process, procedures, etc. ...)
3. Internal controls implementation/operational evidence (control tests or evidence showing execution of the internal controls indicated)

Please indicate in this table:

|  |  |
| --- | --- |
| **All Internal Control(s) related to CIP-009-6 - R2** | |
| **Global Program Filename(s)** |  |
| **Comments** |  |
| **Internal Controls Design Filename(s)** |  |
| **Comments** |  |
| **Internal Controls Implementation and/or Operational Evidence Filename(s)** |  |
| **Comments** |  |

***Option 2:***

The following questions may be used as an optional approach to address internal controls for CIP-009-6, R2.

*Note: These questions are similar to those used by MRO in audit engagements. If a process or the implementation is not documented, provide comments of internal control(s) and indicate “not applicable” in supporting evidence fields.*

1. Requirement 2.1
   1. How do you track testing?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. How do you ensure the timeframes for testing and updates are monitored and shared with appropriate stakeholders?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. Requirement 2.2
   1. Have you defined a process or criterion for identifying a representative sample used for testing?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. How do you ensure you have identified and considered all relevant legal and regulatory requirements in your sampling strategy?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. Requirement 2.3

How have you defined an operational exercise?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. If there are internal controls that are not addressed in the internal control questions above for CIP-009-6, R2, please explain in detail and provide supporting evidence if available.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence of Process Filename(s)** |  |
| **Supporting Evidence of Implementation Filename(s)** |  |

Was each question in **R2 Step 1** to **R2 Step 3** shown to follow the appropriate procedure/process?

☐ Yes, respond “Compliant” for R2 to the Self-Certification in Align. Include a comment summary and upload supporting documentation to the ERO SEL.

☐ No, respond “Not Compliant” for R2 to the Self-Certification in Align. Include a comment summary based on potential issues and upload supporting documentation to the ERO SEL.

☐ Do not own, respond “Do Not Own” for R2 to the Self-Certification in Align. Include comments supporting the “Do Not Own” response and upload supporting documentation to the ERO SEL.

☐ Do not meet the applicability requirements of the full standard, respond “Not Applicable” for R2 to the Self-Certification in Align. Include comments supporting the “Not Applicable” response and upload supporting documentation to the ERO SEL. This response should not be used if the circumstance within the standard or requirement language did not happen. This response should only be used if the requirement or standard is not applicable at all to the entity (such as not registered for the function).

# 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. Evidence supporting the Internal Control Option 1 or Option 2 for each requirement.

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 response 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.