**[Registered Entity Name]**

**NERC ID: [NCRXXXXX]**

**CIP-007-6 – Cyber Security – Systems Security Management, R3**

**3rd 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) Site:
   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-007-6 – Cyber Security – Systems Security Management**

***R3.*** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention.*

***M3.*** Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

***3.1.***Deploy method(s) to deter, detect, or prevent malicious code.

***M3.1.***An example of evidence may include, but is not limited to, records of the Responsible Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

***3.2.***Mitigate the threat of detected malicious code.

***M3.2.***Examples of evidence may include, but are not limited to:

• Records of response processes for malicious code detection

• Records of the performance of these processes when malicious code is detected.

***3.3.***For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

***M3.3.*** An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

# Purpose:

# To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

# 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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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.
        3. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

## Generator Operator

* + - 1. **Generator Owner**
      2. **Interchange Coordinator or Interchange Authority**
      3. **Reliability Coordinator**
      4. **Transmission Operator**
      5. **Transmission Owner**

# Assessment Guidance

1. Provide each documented process that collectively addresses each of the applicable requirement parts in CIP-007 R3.

|  |  |
| --- | --- |
| **Process Document(s) Requested** | |
| **Filename(s)** |  |
| **Comments** |  |

1. For each instance(s) of detected malicious code during the monitoring period, provide evidence the threat of the detected malicious code was mitigated. Indicate N/A in table below, if there was no instance(s) of detected malicious code during the monitoring period.

|  |  |
| --- | --- |
| **Detected Malicious Code Document(s) Requested** | |
| **Filename(s)** |  |
| **Comments** |  |

1. Provide a list of all the methods(s) utilized to deter, detect, or prevent malicious code.

|  |  |
| --- | --- |
| **Malicious Code Methods(s) Requested** | |
| **List** |  |
| **Comments** |  |

1. For each method documented in step #3, provide system-generated evidence (generated no more than 60 days from self-certification submittal date) demonstrating deployment. If the list provided in step #3 is greater than 20, please provide a judgmental sample of the list provided in step #3 to include 20 methods.

|  |  |
| --- | --- |
| **Malicious Code Tool(s) Evidence Requested** | |
| **Filename** |  |
| **Comments** |  |

1. For each method documented in step #3, provide evidence (generated no more than 60 days from self-certification submittal date) demonstrating that updating, testing, and installation of signatures or patterns are utilized, where applicable. Indicate N/A in table below, if methods utilized do not include signature or pattern utilization. If the list provided in step #3 is greater than 20, please provide a judgmental sample of the list provided in step #3 to include 20 methods.

|  |  |
| --- | --- |
| **Signature and Pattern Evidence Requested** | |
| **Filename** |  |
| **Comments** |  |

**Internal Control(s) – Required (Provide information for either Section 1 or Section 2):**

The internal controls sections provided are meant to allow entities to decide the best approach to provide their internal control information. Section 1 is meant to allow registered entities to provide their information as they see applicable and in their format. Section 2 is meant to help registered entities

Section 1:

The following section is being utilized to gather internal control information. Provide information that shows:

1. Internal controls incorporation into global program for CIP-007-6 R3
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-007-6 R3** | |
| **Global Program Filename** |  |
| **Comments** |  |
| **Internal Controls Design** |  |
| **Comments** |  |
| **Internal Controls Implementation and/or Operational Evidence** |  |
| **Comments** |  |

Section 2:

The following questions can be used as an optional approach to address internal controls for CIP-007-6 R3. Note: These questions are similar to those used by MRO in audit engagements.

1. Explain in detail, how does Entity ensure anti-malware software updates corresponding to the scanning engine and signature database on a regular basis

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail, does Entity enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail, does Entity send all malware detection events to anti-malware administration tools and/or event log servers for analysis and alerting?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail, does Entity enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail, does Entity enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail what system(s) are used to generate alerts and/or alarms of malicious code.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail if tests, such as EICAR, are utilized.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail if the method for detecting known or suspected malicious communications (CIP-005 R1 Part 1.5) was identified as a method for the purpose of CIP-007 R3 Part 3.1.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. If applicable, explain in detail, how the statement of no detection of malicious code can be substantiated.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

1. Explain in detail if there are additional steps taken to ensure updating, testing, and installation of signature or patterns for the method(s) used for detecting known or suspected malicious communications.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence** |  |

Was there sufficient evidence supplied for steps #1 - #5 for the purpose of CIP-007 R3?

☐ Yes, respond “Compliant” for R3 to the Self-Certification in Align. Include a comment summary and upload supporting documentation to the SEL site.

☐ No, respond “Not Compliant” for R3 to the Self-Certification in Align. Include a comment summary based on potential issues and upload supporting documentation to the SEL site.

☐ Do not own, respond “Do Not Own” for R3 to the Self-Certification in Align. Include comments supporting the “Do Not Own” response and upload supporting documentation to the SEL site.

☐ Do not meet the applicability requirements of the full standard, respond “Not Applicable” for R3 to the Self-Certification in Align. Include comments supporting the “Not Applicable” response and upload supporting documentation to the SEL site. 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 section 1 or section 2

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.